



Chapter 5: Wireless PANs

Table of Contents

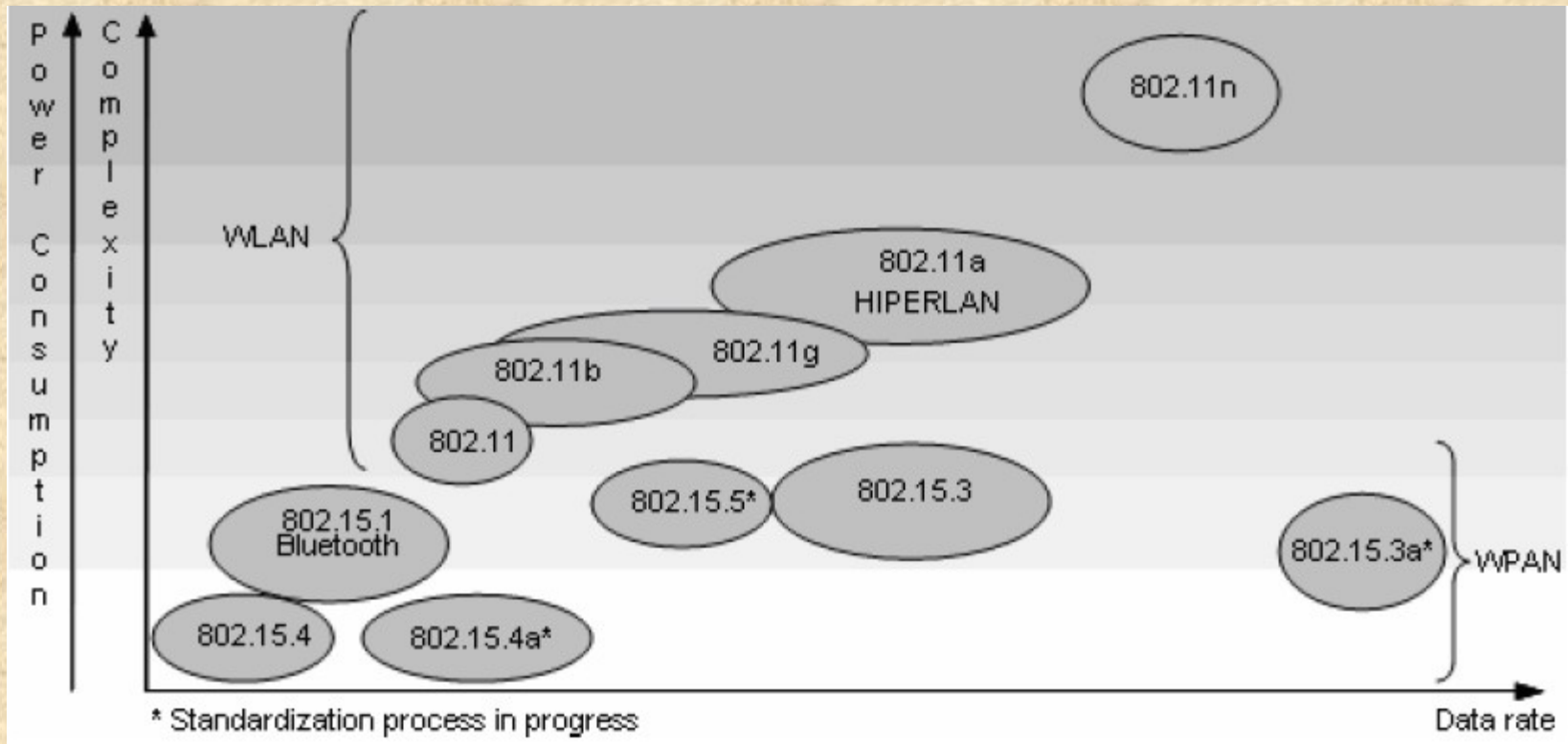
- Introduction
- Why Wireless PANs
- The Bluetooth Technology
 - History and Applications
 - Technical Overview
 - The Bluetooth Specifications
 - Piconet Synchronization and Bluetooth Clocks
 - Master-Slave Switch
 - Bluetooth Security
- Enhancements to Bluetooth
 - Bluetooth Interference Issues
 - Intra and Inter Piconet Scheduling
 - Bridge Selection
 - Traffic Engineering
 - QoS and Dynamic Slot Assignment
 - Scatternet Formation
- The IEEE 802.15 Working Group for WPANs
 - The IEEE 802.15.3
 - The IEEE 802.15.4
- Comparison between WPAN Systems
 - Range
 - Data Rate
 - Support for Voice
 - Support for LAN Integration
 - Power Management
 - Comparison and Summary of Results
- WLANs versus WPANs
- Conclusion and Future Directions



Introduction

- WPANs are short to very-short range wireless networks (from a couple centimeters to a couple of meters)
- WPANs can be used to replace cables between computers and their peripherals
- The IEEE 802 has established the IEEE 802.15 WG for WPANs, which standardizes protocols and interfaces for WPANs
- The best example representing WPANs is the industry standard Bluetooth, which can be found in many consumer electronics
- Other less popular examples of WPAN technologies include Spike, IrDA and in the broad sense HomeRF

WLAN and WPAN Standards



Note: As of March 2006, the 802.15.3a task group has been officially withdrawn from the IEEE

Operating space of the various IEEE 802 WLAN and WPAN standards and other activities still in progress



Why Wireless PANs

- The concept of Personal Area Networks (PANs) was first demonstrated by IBM researchers in 1996 that utilized human body to exchange digital information
- IBM engineers created a way to communicate between body-borne appliances by using the human body as a channel, with the only limitation of some form of human contact between devices is required which may not always be desirable or possible
- To get around this problem of human contact, other alternatives such as infrared (IR) or far-field (radio) communications have been considered, using wireless methods such as IR or radio frequency (RF) for PANs
- WPAN devices are typically smaller, operate on battery power, and are either worn on a human body or carried personally
- The main design goal of WPANs is to allow devices that are in close proximity to communicate and exchange information with each other, either stationary or moving
- A WPAN is **functionally** similar to a WLAN, while differs in terms of power consumption, coverage range, data rate and the cost



Why Wireless PANs

- WPAN should allow devices to create or provide data/voice access points, personal ad hoc connectivity and be a replacement for having connecting cables
- The operating range for these devices is within a personal operating space (POS) of up to 10 meters in all directions, and envelops a stationary or a mobile person
- The concept of a POS can also be extended to devices such as printers, scanners, digital cameras, microwave ovens, TVs or VCRs
- The WPAN systems are expected to provide secure modes of operation, allowing groups of personal devices to interconnect while excluding connectivity to other non-essentials
- They should not affect the primary function, the form factor and power consumption of the devices in which they are embedded
- As WPANs use the license-free radio frequencies (e.g., ISM band), they have to coexist with other RF technologies that make use of these frequencies



The Bluetooth Technology

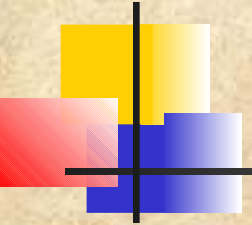
- Bluetooth (or simply BT) has been a topic of considerable buzz in the telecommunications industry for the past few years
- Bluetooth is named after a **10th-century Viking king** known for his success in uniting Denmark and Norway during his rule around 960 AD
- Bluetooth is a low cost and short-range radio communication standard that was introduced as an idea in Ericsson Laboratories back in 1994
- Engineers envisioned a need for a wireless transmission technology that would be cheap, robust, flexible, and consume low power
- Bluetooth was chosen to serve as the baseline of the IEEE 802.15.1 standard for WPANs, which can support both synchronous traffic such as voice, and asynchronous data communication



Applications of Bluetooth

Some application areas where Bluetooth networks could be explored

- **Consumer – Wireless PC peripherals, smart house wireless PC peripherals, smart house integration, etc.**
- **Games – Controllers, virtual reality, iPODs, etc.**
- **Professional – Pagers, PDAs, cell phones, desktops, automobiles, etc.**
- **Services – Shipping, travel, hotels, etc.**
- **Industry – Delivery (e.g., scanners, printers), assembly lines, inspections, inventory control, etc.**
- **Sports training – Health sensors, monitors, motion tracking, etc.**
- **Military – Combat and maintenance**



Bluetooth – Technical Overview

- The Bluetooth Specification (version 1.1) describes radio devices designed to operate over very short ranges – on the order of **10 meters** – or optionally a medium range (100 meters) radio link capable of voice or data transmission to a maximum capacity of **720 kbps** per channel (with a nominal throughput of 1 Mbps)
- Radio frequency operation is in the unlicensed ISM band at **2.4 to 2.48 GHz**, using a frequency hopping spread spectrum (FHSS), full-duplex signal at up to 1600 hops/seconds
- The Bluetooth specifications are divided into two parts:
 - *The Core* – This portion specifies components such as the radio, base band (medium access), link manager, service discovery protocol, transport layer, and interoperability with different communication protocols
 - *The Profile* – The Profile portion specifies the protocols and procedures required for different types of Bluetooth applications

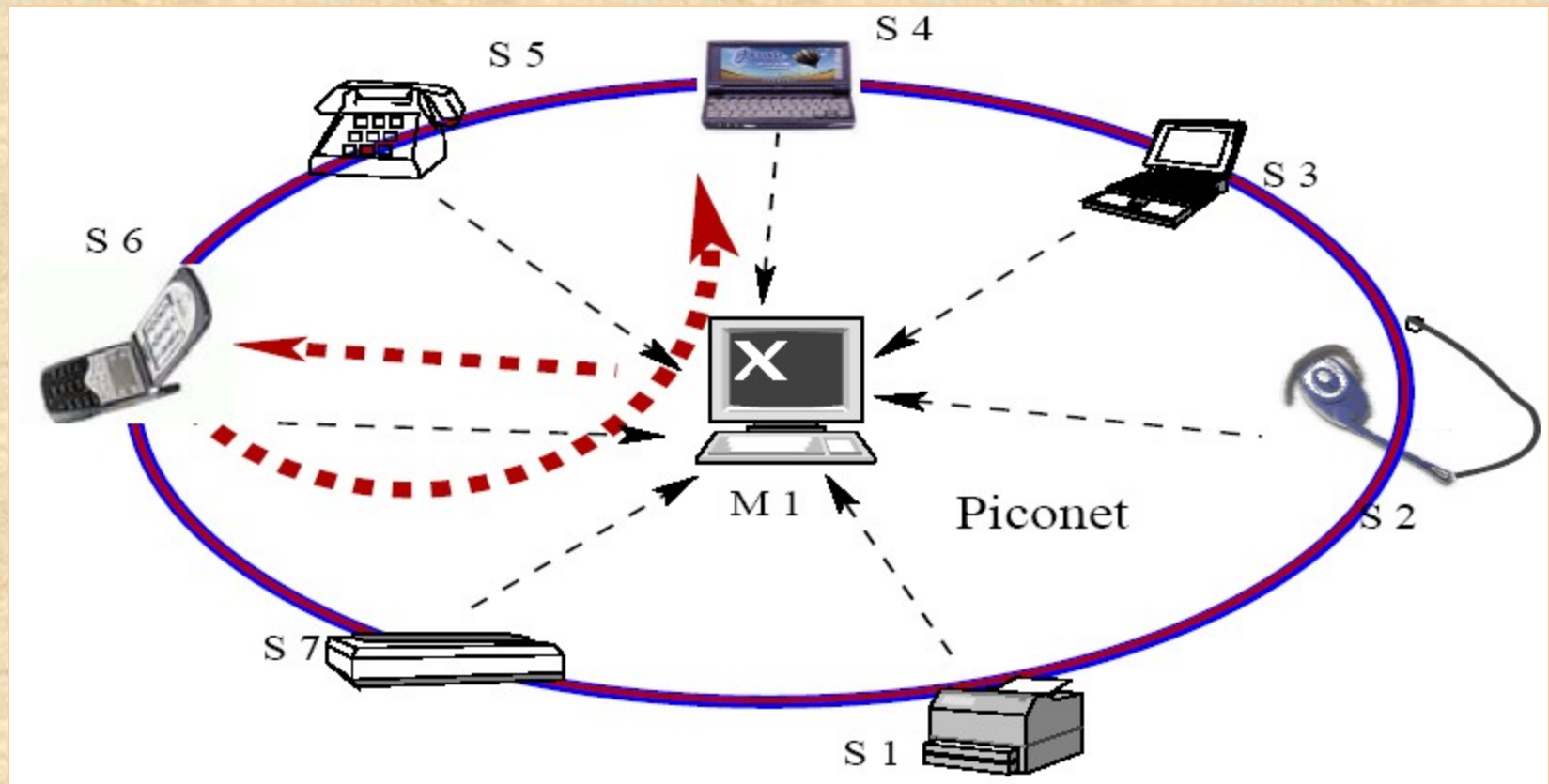


Bluetooth – Technical

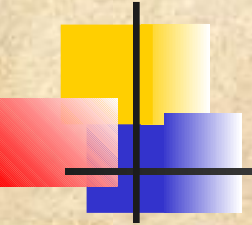
Overview

- Whenever a pair or small group of Bluetooth devices come within radio range of each other, they can form an ad hoc network without requiring any infrastructure
- Devices are added or removed from the network dynamically and they can connect to or disconnect from an existing network at will and without interruption to the other participants
- In Bluetooth, the device taking the initiative to start communication to another device assumes the role of a *master*, while the recipient becomes a *slave*
- The basic architectural unit of a Bluetooth is a *Pico net*, composed of one master device and up to seven active *slave devices*, which can communicate with each other only through their master

Bluetooth Piconet



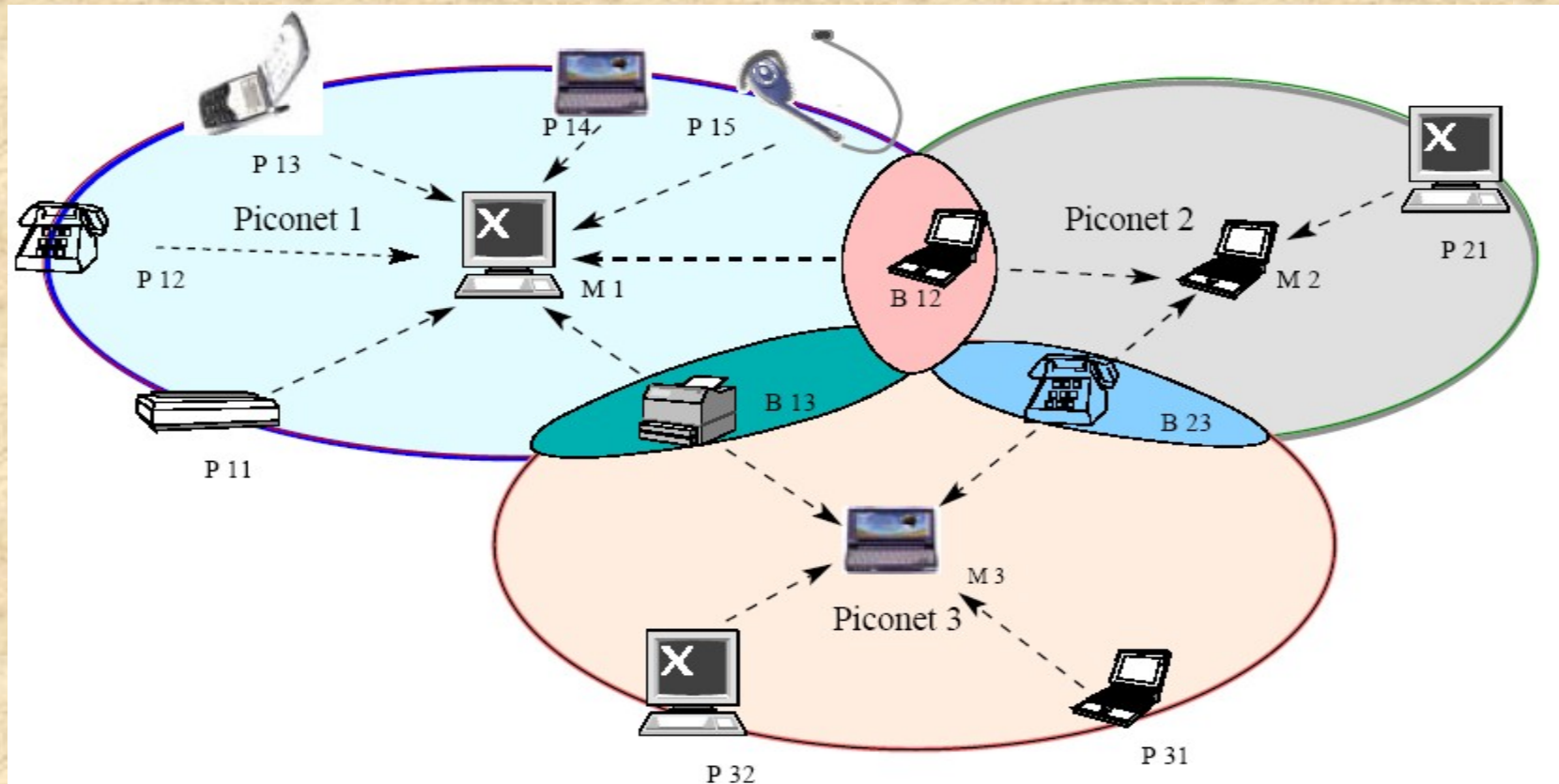
An example of a Piconet



Bluetooth – Technical Overview

- Every Bluetooth device is exactly the same except for a 48-bit device identifier (BD_ADDR)
- Besides up to **7- active** slaves, additional devices can be connected to a Piconet in a parked state in which they listen but do not participate
- When they want to participate, they are swapped in and one of the active devices is swapped out
- If the acting master leaves the Pico net, one of the slaves assumes its role
- With this method, up to **255** devices can be virtually connected to the Piconet
- Also, each piconet uses a different Frequency Hopping Sequence (FHS) in order to reduce interference with other nearby piconets
- To increase the number of devices in the network, a *scatternet* architecture consisting of several piconets has been proposed

Bluetooth Scatternet



- A scatternet comprised of three piconets
- Since scatternets span more than a single piconet, therefore a few nodes act as **bridges** (e.g., B12, B13, B23) responsible for relaying packets across piconet boundaries



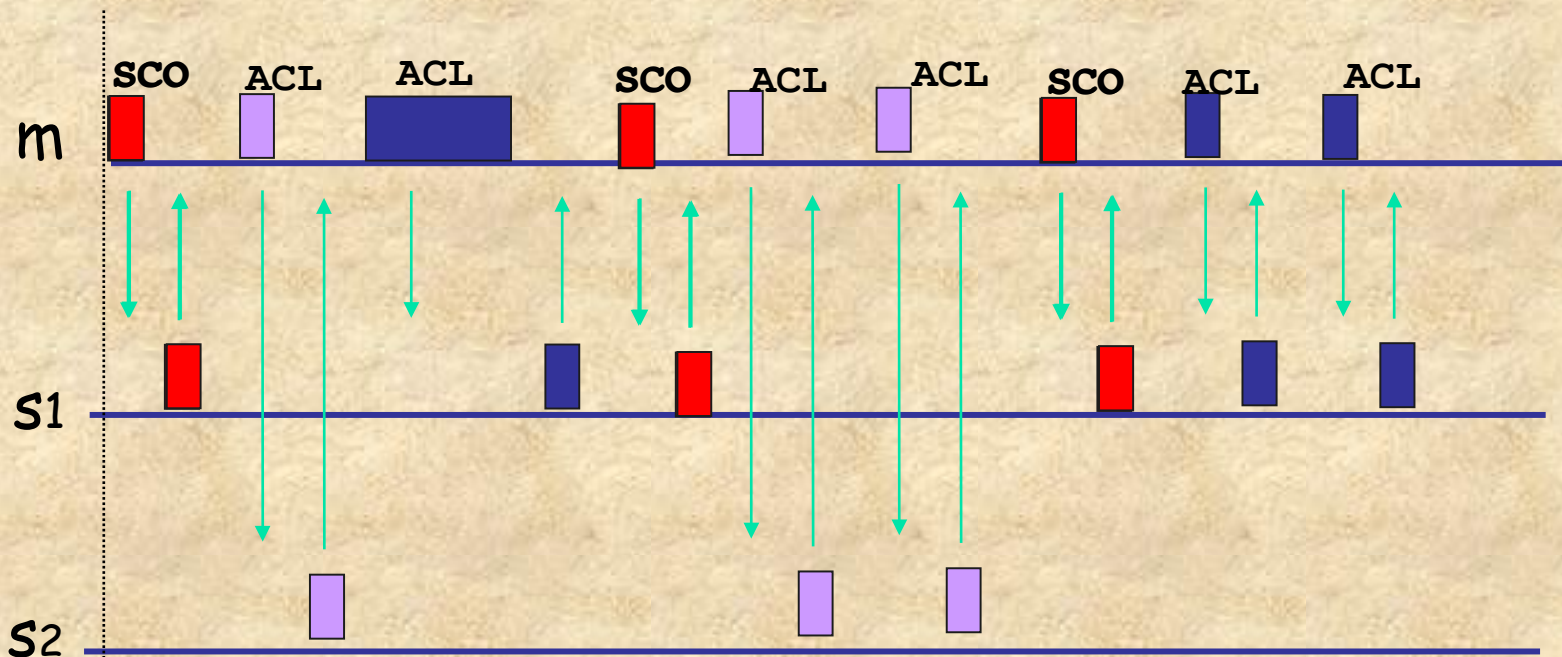
Bluetooth – Technical

Overview

- The Bluetooth specification defines two different types of links for data and voice applications:
- The Synchronous Connection Oriented (SCO) link
 - SCO link is a symmetric, point-to-point link between the master and one slave
 - Usually, the SCO link is used for audio applications with strict Quality of Service (QoS) requirements
- The Asynchronous Connectionless (ACL) link
 - ACL link is treated as a packet switched, point to point and point to multipoint data traffic link
- The master maintains one ACL link with each active slave over which upper layer connection can be established and re-transmission is employed only when it is necessary to ensure the data integrity

Physical Link Types

- Synchronous Connection Oriented (SCO) Link
 - Slot reservation at fixed intervals
- Asynchronous Connection-less (ACL) Link
 - Polling access method



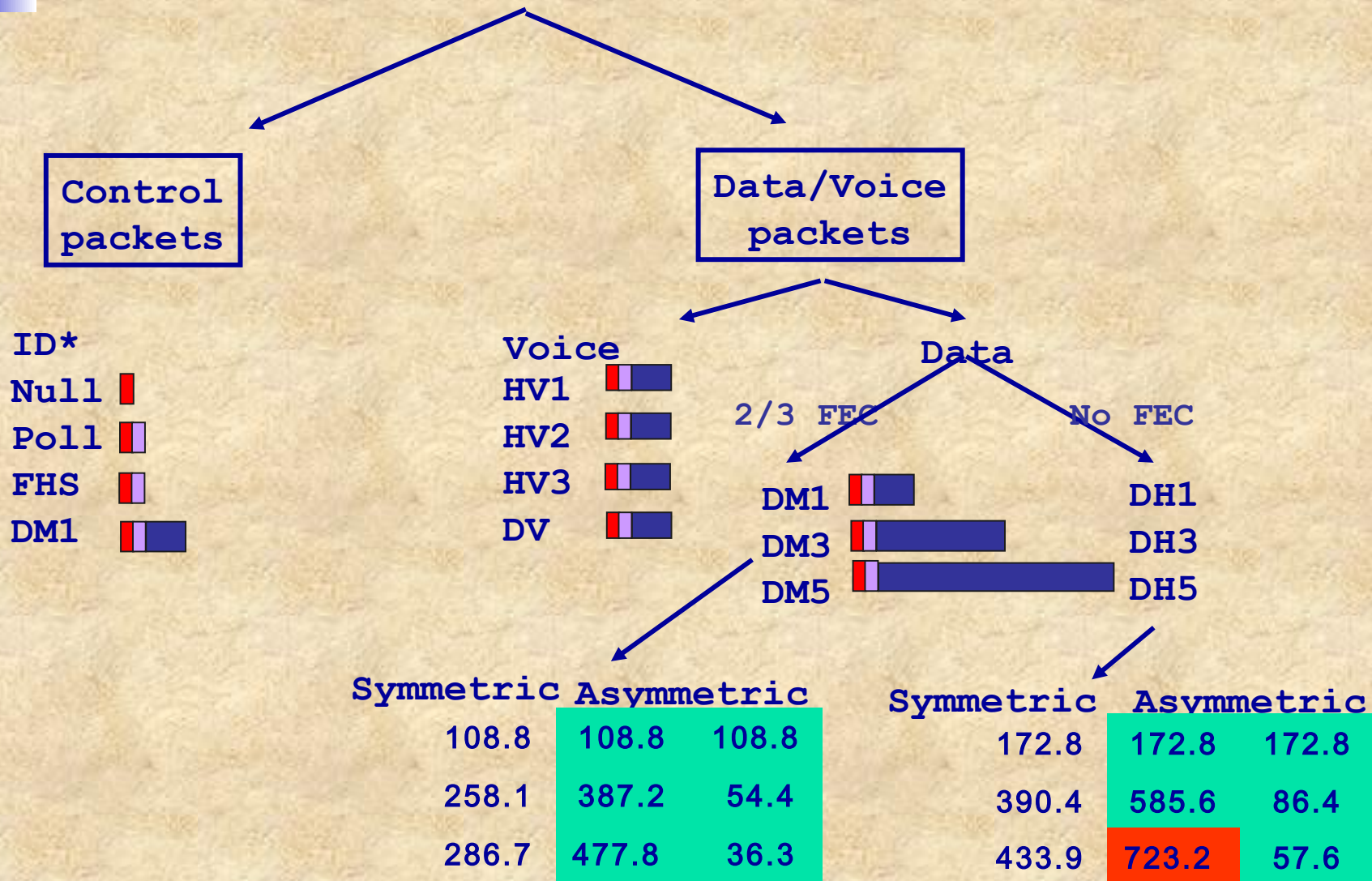


Bluetooth packet types

Type	User Payload (bytes)	FEC	Symmetric (Kbps)	Assymetric (Kbps)	Assymetric (kbps)
DM1	0-17	Yes	108.0	108.0	108.0
DH1	0-27	No	172.8	172.8	172.8
DM3	0-121	Yes	256.0	384.0	54.4
DH3	0-183	No	384.0	576.0	86.4
DM5	0-224	Yes	286.7	477.8	36.3
DH5	0-339	No	432.6	721.0	57.6
HV1	0-10	Yes	64.0	-	-
HV3	0-20	Yes	128.0	-	-
HV5	0-30	No	192.0	-	-

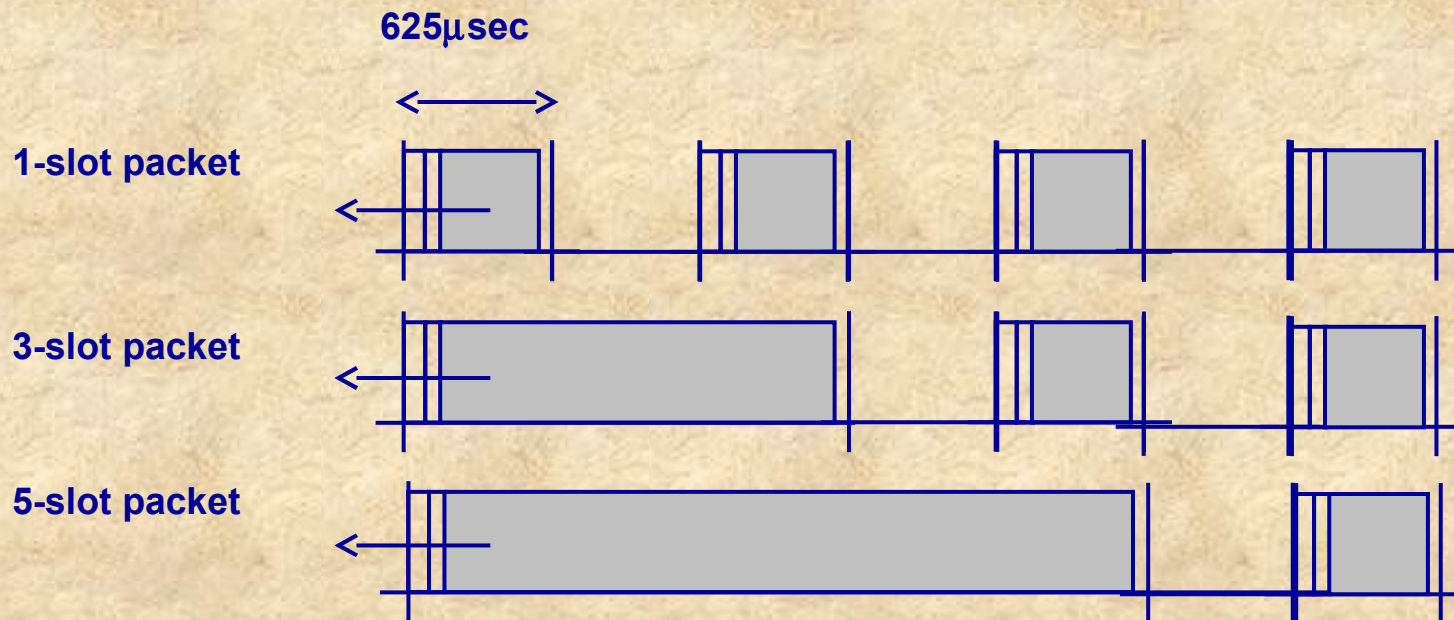
- Considering its nominal 1 Mbps piconet bandwidth and the 64 Kbps requirement for a SCO connection, it will be clear later that a Bluetooth piconet can support up to three simplex SCO links (when using HV3 packets) so as to meet the required QoS needs
- This can be easily concluded based on the numbers given in the Table

Packet Types and Bandwidth



Packet transmission in Bluetooth

- Bluetooth defines a set of types of packets, and information can travel in these packet types only
- Bluetooth allows the use of 1, 3 and 5 slot packets as depicted below





Packet transmission in Bluetooth

- A TDD scheme divides the channel into $625 \mu\text{ sec}$ slots at a 1 Mb/s rate
- As a result, at most 625 bits can be transmitted in a single slot
- However, **to change** the Bluetooth device from transmit state to receive state and tune to the next frequency hop, a **$259 \mu\text{ sec}$** turn around time is kept at the end of the last slot
- This results in reduction of effective bandwidth available for data transfer
- Bluetooth employs HVx (High-quality Voice) packets for SCO transmissions and DMx (Data Medium-rate) or DHx (Data High-rate) packets for ACL data transmissions, where $x = 1, 3 \text{ or } 5$

Connection Setup in Bluetooth

- Connection setup in Bluetooth starts with each node discovering its neighbors and this process is called *inquiry*



- For two devices to discover each other, while one of them is in INQUIRY state, the other has to be in INQUIRY SCAN
- The node in INQUIRY SCAN responds to the INQUIRY of the other node
- This way the node in INQUIRY state notices the presence of the node in INQUIRY SCAN
- When the devices want to build up a connection, they begin the *page* procedure
- Similar to the inquiry phase, there are two states: PAGE and PAGE SCAN
- When one of the nodes wants to build up a connection to the other node, it enters in the PAGE state and when the other node enters PAGE SCAN state, the connection setup is concluded



Bluetooth – Specifications

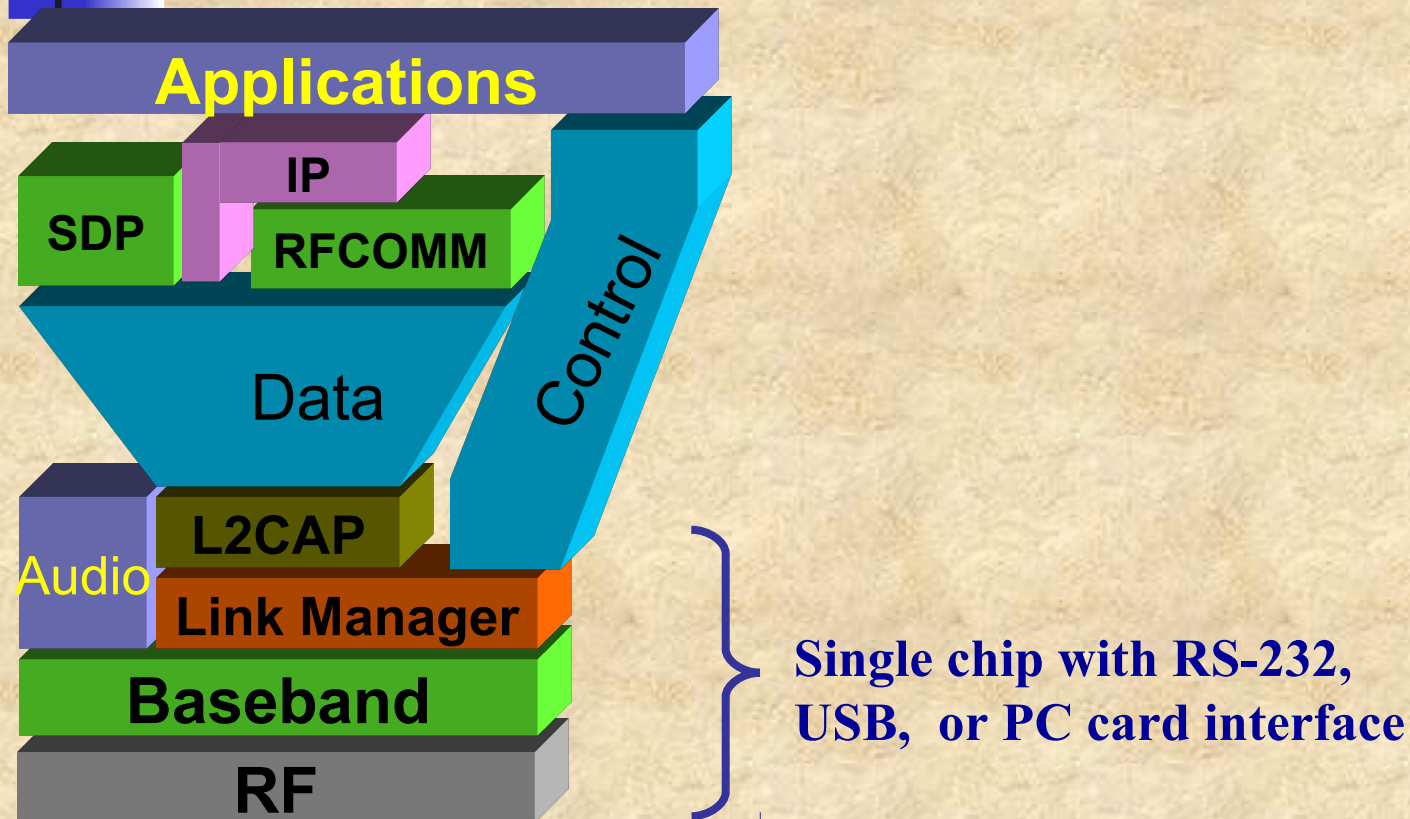
The Bluetooth Specifications include the following

- 1. The Protocol Stack core functionality**
- 2. The usage Profiles for different applications**

Protocol Stack (Figure on next slide)

- **The stack defines all layers unique to the Bluetooth technology**
- **Bluetooth core Specifications only define the Physical and the Data Link layers of the OSI Protocol Stack**
- **The application layer shown in Figure 5.6 (on next slide) actually includes all the upper layers (IP, Transport, Application) sitting on the RFCOMM and the SDP**
- **These layers are not themselves part of the stack and this host stack are handled in software**
- **They communicate with lower layers via the Host Controller and the lower layers (RF, Baseband and LMP) are built in hardware modules**

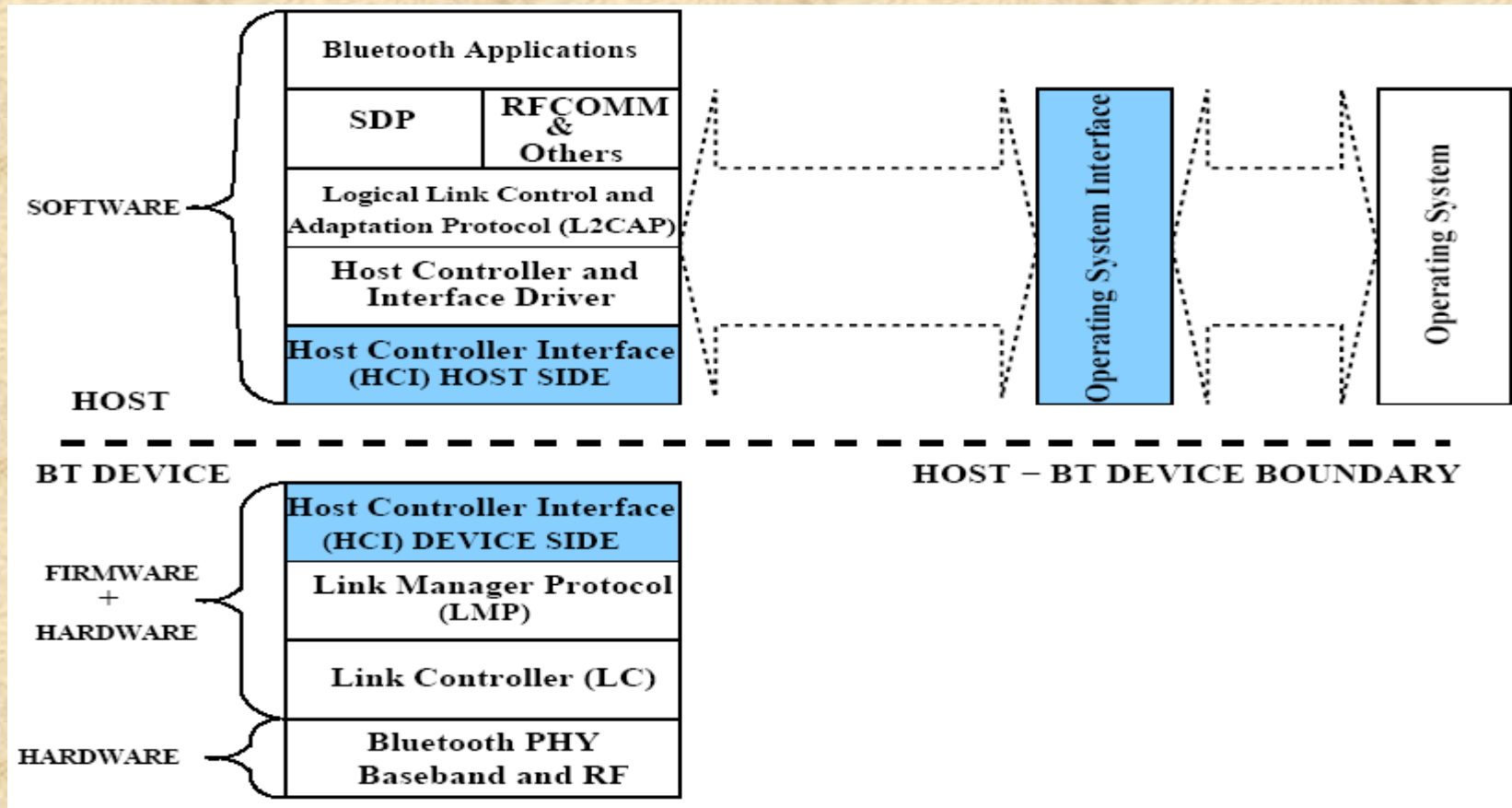
Bluetooth Specifications



A hardware/software/protocol description

An application framework

Layered structure of Bluetooth Protocol Stack





Bluetooth Specifications- Radio Layer

- The radio layer, which resides below the Baseband layer, defines the technical characteristics of the Bluetooth radios
- It is the lowest layer in Bluetooth protocol stack and it defines the requirements of Bluetooth transceivers operating in unlicensed ISM band
- Currently, many other wireless devices operate in this band and, as covered in later chapters, this creates interference
- Bluetooth mitigates this effect using FHSS as it also uses FEC to reduce the impact of noise on long distance links
- It has a nominal range of **10 meters at a 0dBm (1 mW)** power setting which can be extended up to **100 meters on a 20 dBm (100 mW)** power setting
- It uses a Binary Frequency Shift Keying (BFSK) modulation technique which represents a binary 1 as a negative frequency deviation



Bluetooth Specifications- *Baseband*

- The baseband defines the key procedures that enable devices to communicate with each other
- In other words, the baseband layer incorporates the MAC procedures of Bluetooth
- It defines how piconets are created, and also determines the packet formats, physical-logical channels and different methods for transferring voice and data
- It provides link set-up and control routines for the layers above
- Additionally, the baseband layer provides lower level encryption mechanisms to provide security to links



Bluetooth Specifications- Link Manager Protocol

- **The Link Manager Protocol (LMP) is a transaction protocol between two link management entities in different Bluetooth devices**
- **LMP messages are used for link setup, link control/configuration and the security aspects like authentication, link-key management and data encryption**
- **It also provides a mechanism for measuring the QoS and the Received Signal Strength Indication (RSSI)**
- **The link manager provides the functionality to attach/detach slaves, switch roles between a master and a slave, and establish ACL/SCO links**
- **Finally, it handles the low power modes hold, sniff and park, designed to save power when the device has no data to send**



Bluetooth Specifications- Host Controller Interface

- **The Host Controller Interface (HCI) provides a uniform command interface to the baseband and the LMP layers, and also to the H/W status and the control registers (i.e., it gives higher-level protocols the possibility to access lower layers)**
- **The transparency allows the HCI to be independent of the physical link between the module and the host**
- **The host application uses the HCI interface to send command packets to the Link Manager, such as setting up a connection or starting an inquiry**
- **The HCI itself resides in firmware on the Bluetooth hardware module**
- **It implements the commands for accessing the baseband, the LMP and the hardware registers, as well as for sending messages upward to the host**



Bluetooth Specifications: Logical Link Control and Adaptation Protocol

- The Logical Link Control and Adaptation Protocol (L2CAP) layer shields the specifics of the lower layers and provides a packet interface to higher layers
- At L2CAP level, the concepts of master and slave devices does not exist anymore as it provides a common base for data communication
- The L2CAP layer supports the higher level protocol multiplexing, packet segmentation and reassembly and QoS maintenance

The RFCOMM

- RFCOMM is a simple transport protocol that provides serial port emulation over the L2CAP protocol, and is intended for cable replacement
- It is used in applications that would otherwise use the serial ports of the device



Bluetooth Specifications- Service Discovery Protocol

- **The Service Discovery Protocol (SDP) is defined to provide Bluetooth entities with methods of finding what services are available from each other**
- **The protocol should be able to determine the properties of any future or present service, of an arbitrary complexity in any operating environment**
- **This is a very important part of Bluetooth technology since the range of services available is expected to grow rapidly as developers bring out new products**



Bluetooth Specifications: Bluetooth Profiles

- A profile is defined as a combination of protocols and procedures that are used by devices to implement specific services as described in the Bluetooth usage models
- For example, the “headset” profile uses AT Commands and the RFCOMM protocol and is one of the profiles used in the “Ultimate Headset” usage model
- Profiles are used to maintain interoperability between devices (i.e., all devices conforming to a specific profile will be interoperable), which is one of the Bluetooth’s primary goals
- Bluetooth has so far specified **four** general profiles and are the generic access profile, the serial port profile, the service discovery application profile, and the generic object exchange profile
- The number of Profiles will continue to grow as new applications come about



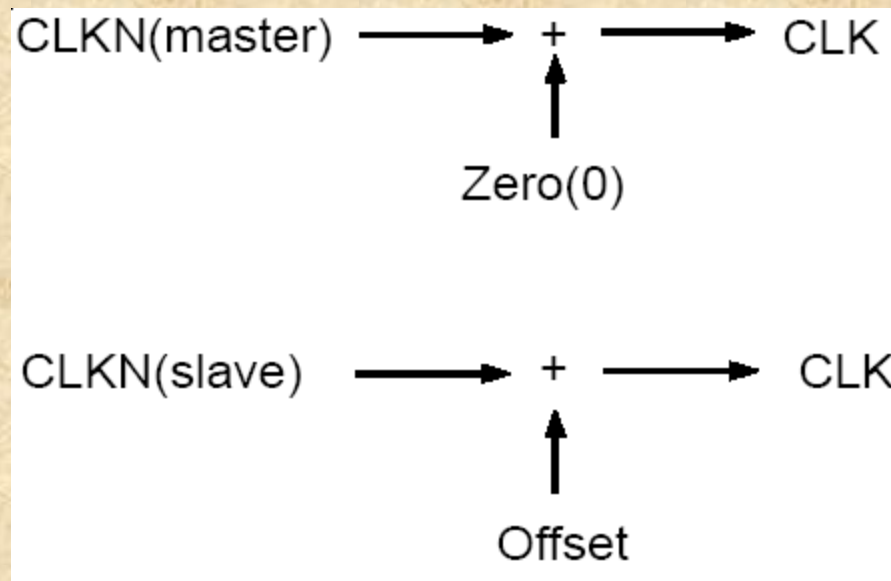
Piconet Synchronization

- Every Bluetooth unit has an internal clock called the native clock (CLKN) and a Bluetooth clock is derived from this free running native clock
- For synchronization with other units, offsets are added to the native clock to obtain temporary Bluetooth clocks (CLK), which are mutually synchronized
- When a piconet is established, the master's native clock is communicated to all its slaves to generate the offset value
- The Master keeps an exact interval of $M \cdot 625 \mu\text{sec}$ (where M is an even, positive integer greater than 0) between consecutive transmissions
- The slave's Rx timing is adjusted with any packet sent in the master-to-slave slot, whereas the slave's Tx timing is adjusted based on the most recent slave Rx timing



Slaves' Derived Clocks

Every slave unit participating in a piconet uses the derived clock (CLK), for all timing and scheduling activities in the piconet





Bluetooth – Master -Slave Switch

- The current Bluetooth specification provides means for a **Master- Slave role switch** (from now on referred to simply as M/S switch)
- This procedure is desirable on occasions such as:
 - When a unit paging the master of an existing piconet wants to join this piconet
 - When a slave in the existing piconet wants to set up a new piconet involving itself as a master, and the current master as a slave
 - When a slave wants to fully take over an existing piconet as a new master
- M/S switching is satisfied in three steps, namely TDD Switch, Piconet Switch for the previous master, and Piconet Switch for the remaining slaves

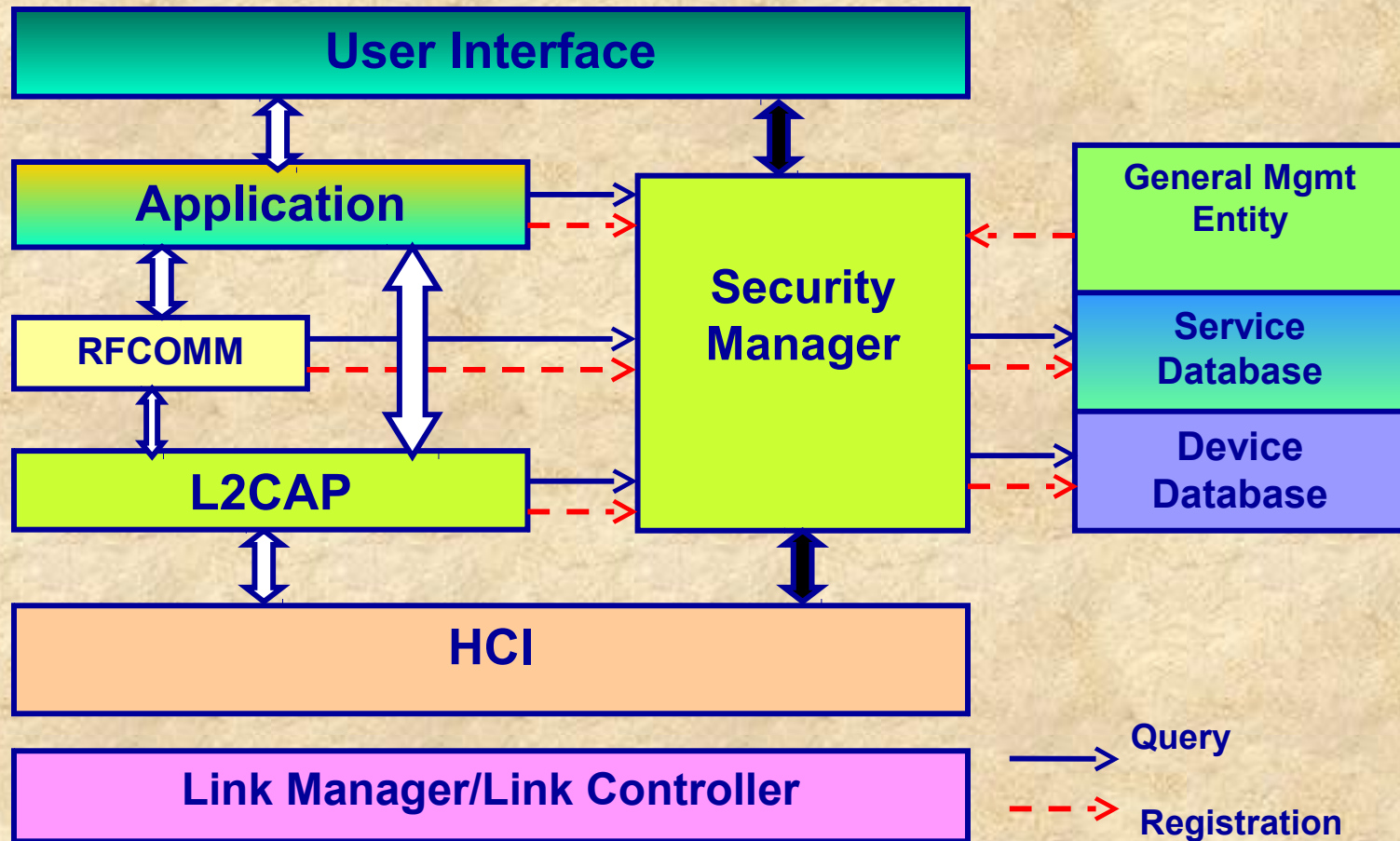


Bluetooth – Security

- Security is an important issue in WPANs
- Bluetooth devices use a combination of the Personal Identification Number (PIN) and a Bluetooth address
- Data encryption can be used to further enhance the degree of Bluetooth security
- Bluetooth uses transmission scheme that provides a level of security in itself
- FHSS alleviates interference as the radio hops between the channels at a fast speed of **1600 hops per second** which provides some level of security on data transmission
- In addition, the low power transmissions prevent the radio signals from propagating too far
- The information on a Bluetooth packet payload is encrypted, and the encryption is carried out with a stream cipher E0, which is synchronized for each payload

Bluetooth – Security Architecture

A high level overview of the Bluetooth security components





Bluetooth – Security

- Security manager stores information about the security of services and devices
- It decides on the acceptance of the access or disconnection and requires authentication and encryption if needed
- Security manager also initiates setting up a trusted relationship and pairing, and handles the PIN code from the user
- Bluetooth has several different security levels that can be defined for devices and services
- The devices can have two trust levels
 - ▣ Trusted - This level requires a fixed and trusted relationship and it has unrestricted access to all the services, as the device has to be previously authenticated
 - ▣ Untrusted - The untrusted device does not have fixed relationship and its access to services is limited, a new device is labeled as unknown device and is always untrusted



Bluetooth – Security Level of Services

- **The security level of a service is defined by three attributes:**
 - ▣ **Authorization required:** Access is only granted automatically to trusted devices or untrusted devices after an authorization procedure
 - ▣ **Authentication required:** Before connecting to the application, the remote device must be authenticated
 - ▣ **Encryption Required:** The link must be changed to encrypted mode, before access to the service is possible
- **On the lowest level, the services can be set to be accessible to all devices**
- **When the highest level of security is needed, the service can require both authorization and authentication and a trusted device has access to the services, but an untrusted device needs manual authorization**



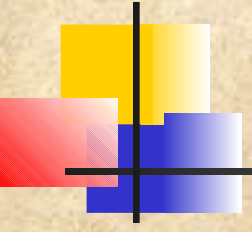
Bluetooth Security- Link Key

- All security transactions between two or more parties are handled by a 128-bit random number, called the **link key**
- Used in the authentication process and as a parameter when deriving the **encryption key**
- Lifetime of a link key depends on whether it is a semi-permanent or a **temporary key**
- A **semi-permanent key** can be used after the current session is over to authenticate Bluetooth units that share
- **Temporary keys** are commonly used in point-to-multipoint connections, where the same information is transmitted to several **recipients**



Bluetooth Security: four link keys

- The unit key, K_A , is derived at the installation of the Bluetooth device for a unit A
- The combination key, K_{AB} , is generated for each new pair of Bluetooth devices and is used when further security is needed
- The master key, K_{MASTER} , is a temporary key used whenever the master device wants to transmit information to more than one device at once
- The initialization key, K_{INIT} , is used in the initialization procedure and is formed from a random number, an L-octet PIN code, and the BD_ADDR of the claimant unit



Bluetooth – Security

Encryption Key

- The encryption key is generated from the current link key, a 96-bit Ciphering Offset Number (COF) and a 128-bit random number
- The COF is based on the Authenticated Ciphering Offset (ACO), which is generated during the authentication process

PIN Code

- The PIN is a number which can be either fixed or selected by the user, and is employed to enhance the security of the system
- The length of the PIN code can vary between **1 and 16 octets** while regular 4-digit code is sufficient for some applications, but enhanced security requirements may need longer codes

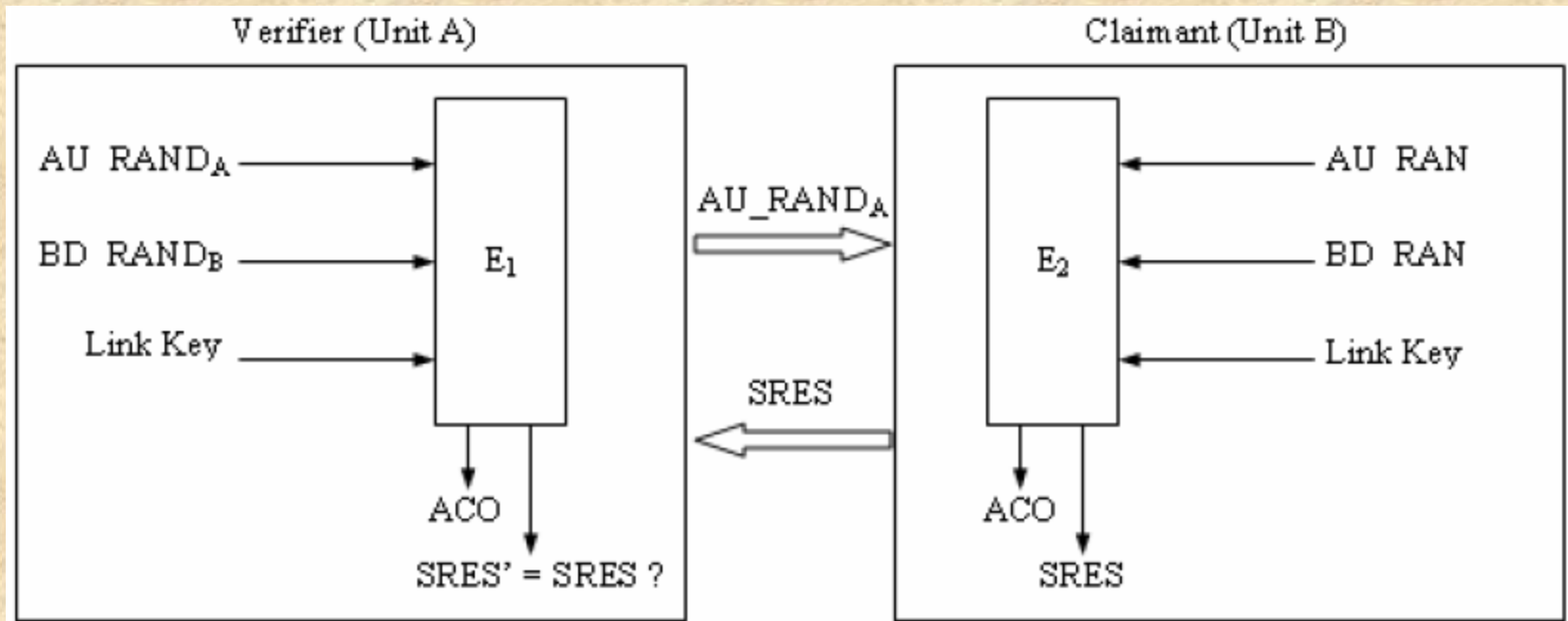


Bluetooth Security:

Authentication

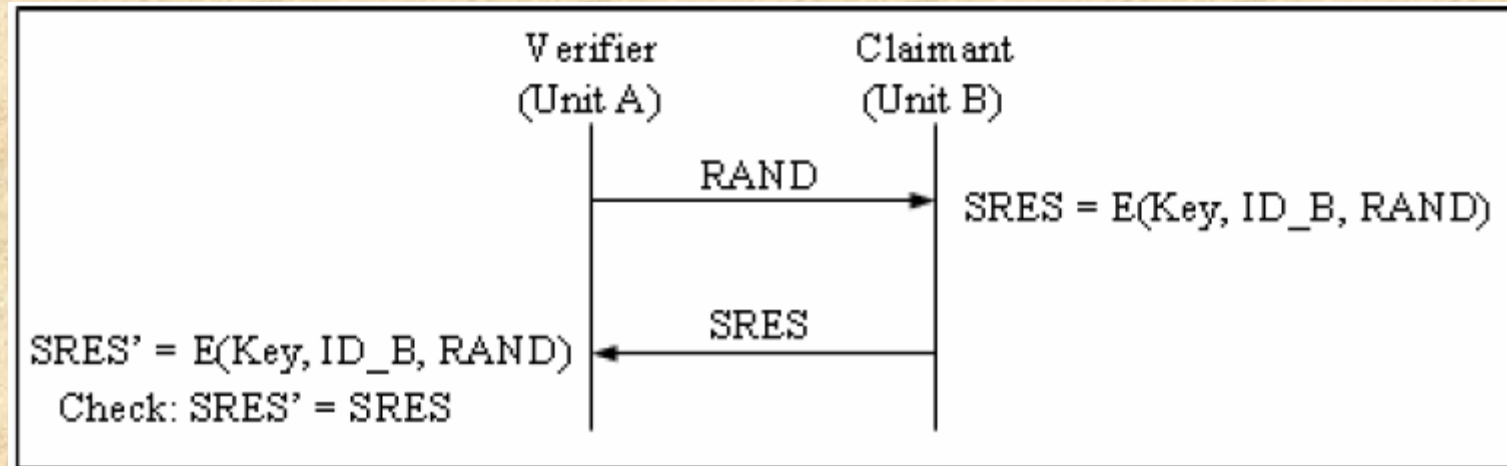
- Authentication starts by issuing a challenge to another device which, in turn, sends a response back which is based on the received challenge, the recipient's BD_ADDR and link key shared between the devices
- Without knowing the PIN, one unit cannot logon to another unit if authentication is activated
- Bluetooth uses a challenge-response scheme in which a claimant's knowledge of a secret key is checked through a 2-move protocol using symmetric secret keys
- As a side product, the **Authenticated Ciphering Offset (ACO)** is computed and stored in both devices and is later used to generate the date encryption key that will be employed between the pair of devices

Challenge Response scheme in Bluetooth



- Unit A sends a random input, denoted by AU_RAND_A (a random number), with an authentication code, denoted by E_1 , to unit B
- Unit B then calculates Signed REsponse (SRES) (shown on the next slide)

Challenge Response scheme in Bluetooth



- Unit B calculates SRES and returns the result to unit A
- Unit A will derive SRES' and will authenticate Unit B if SRES and SRES' are the same



Bluetooth Security:

Limitations

- From the security point of view, Bluetooth has its limitations and supported solutions are not totally satisfactory
- First, the authentication scheme only authenticates the device, not the user and if this feature is needed, it has to be accomplished with the assistance of some application level security mechanism
- Second, Bluetooth does not define a separate authorization for each service and can be applied in the Bluetooth architecture without changing the protocol stack, but changes in the security manager and the registration processes would be necessary
- Presently, Bluetooth allows access control only at connection set up and the access check can be asymmetric, but once a connection is established, data flow is bi-directional in principle and there is no way to enforce unidirectional traffic



Bluetooth Interference Issues

- The 2.4 GHZ ISM band is a broad, free and unlicensed spectrum space used in microwave ovens, cordless phones, remote controllers, as well as Bluetooth and IEEE 802.11b/g devices
- Therefore, all of these inventions have potential of interfering with each other
- Bluetooth uses **much lower** transmission power than IEEE 802.11b as powerful IEEE 802.11b devices may overwhelm its signal
- To address this issue, the Task Group 2 within the IEEE 802.15 working group has been established to improve the coexistence of the two standards



IEEE Efforts to Ensure Coexistence

- **Coexistence** is defined as the ability of one system to perform a task in a given shared environment where other systems may or may not be using the same set of rules
- These practices fall into two categories:
 - **Collaborative:** A collaborative coexistence mechanism is defined as one in which the WPAN and the WLAN communicate and collaborate to minimize mutual interference.
 - **Non-collaborative:** A non-collaborative coexistence mechanism is one wherein there is no method for the WPAN and WLAN to communicate



Inter-Piconet Interference (Intermittent Interference)

- With increasing scalability requirements, the number of co-located piconets will eventually be so large that Bluetooth piconets will now start to interfere with each other
- The FHSS technique with **79** channels employed by Bluetooth will no longer suffice to keep interference at desired minimum levels, and the presence of multiple piconets in vicinity will create interference on signal reception.
- Therefore, not only it is important to qualify and quantify such interference, but it also crucial to propose new ways to mitigate such negative effects



DHx Throughput With/Without Interference (in Kbps)

	Ideal Conditions	Without Interference	With Interference
DH1	172.80	166.66	120.78
DH3	384.00	373.32	329.40
DH5	432.60	417.24	373.32

- A quick evaluation of the Table indicates that results are in line with the ideal ones when there is no interference
- In presence of interference, a drop of more than **30%** in throughput is observed in DH1 links and lower throughput is experienced in all cases, reinforcing a need for tailoring applications closer to these working conditions



Interference Aware Packet Segmentation Algorithm

- The Bluetooth standard defines various packet types to adjust according to different application requirements
- Those **range** from single unprotected 1-slot packet to FEC (Forward Error Correction) encoded 5-slot packets
- Ideally, the adaptation layer should choose the best suitable packet for transmission based both on the application requirements and on the wireless channel condition
- Furthermore, this choice cannot be static for the entire message due to the dynamic nature of error rate in a wireless channel
- Motivated by these issues, an interference-aware algorithm called IBLUES (Interference-aware BLUEtooth Segmentation) has been proposed to dynamically switch between Bluetooth packet types as packet error rates increases or decreases



Overlap Avoidance Schemes

- Two mechanisms, called overlap avoidance (OLA) schemes, have been proposed which are based on traffic scheduling techniques at the MAC layer
- The first mechanism, denoted as voice OLA (V-OLA), is to be performed for the IEEE 802.11b in the presence of a Bluetooth voice (SCO) link
- This scheme avoids overlap in time between the Bluetooth SCO traffic and IEEE 802.11b packets by performing a proper scheduling of the traffic transmissions at the IEEE 802.11b stations
- In a Bluetooth network, each SCO link occupies FH/TDD channel slots according to a deterministic pattern and the station shall start transmitting when the Bluetooth channel is idle by adjusting length of WLAN packet so that it fits between two successive Bluetooth transmissions



Overlap Avoidance Schemes

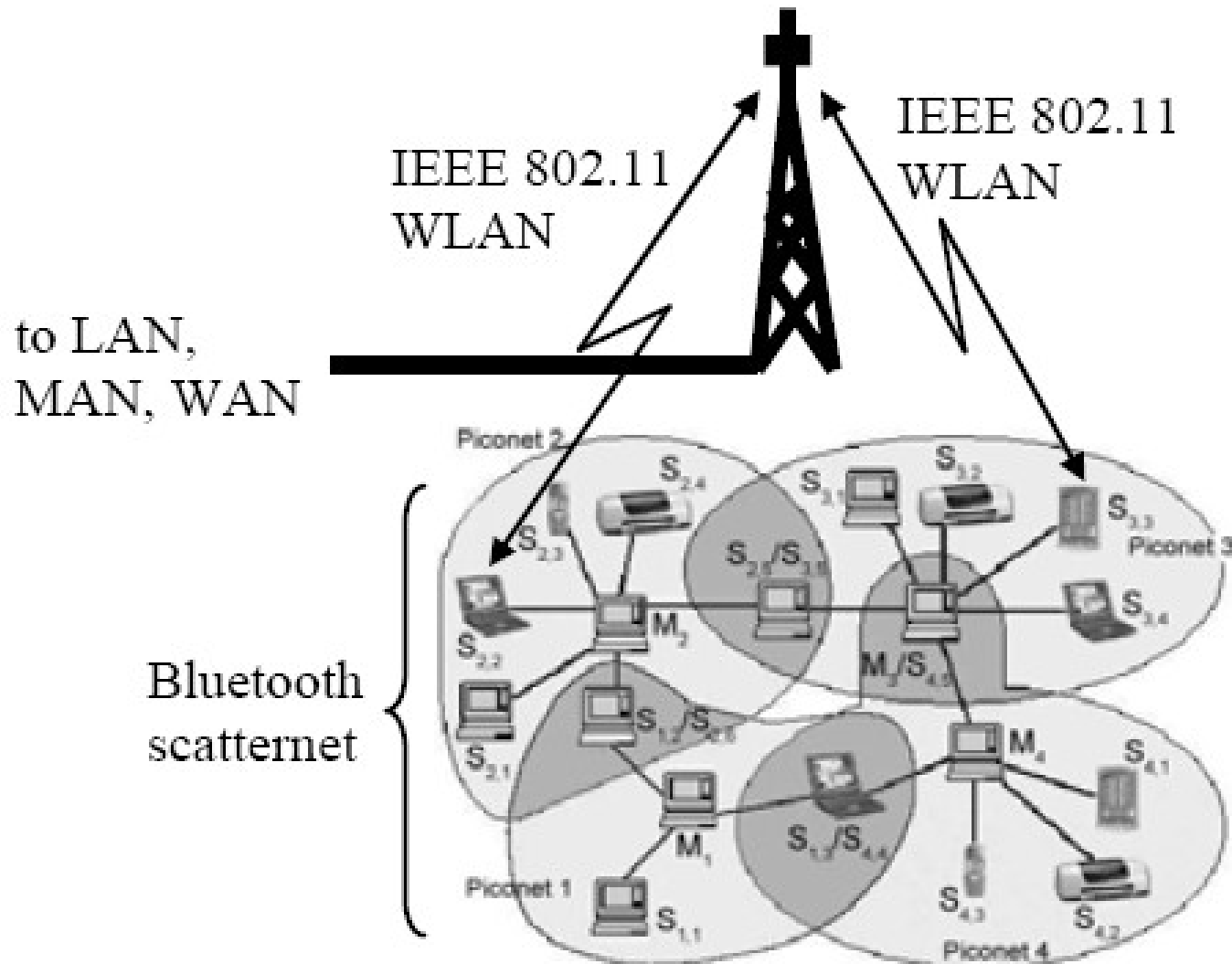
- The second algorithm, denoted by data OLA (D-OLA), is to be performed at the Bluetooth system in case of a Bluetooth data link
- As we have discussed before, the length of a Bluetooth data packet can vary from 1 thru 5 time slots
- In case of multi-slot transmissions, packets are sent by using a single frequency hop which is the hop corresponding to the slot at which the packet started
- The key idea of the D-OLA scheme is to use the variety of packet lengths that characterize the Bluetooth system so as to avoid overlap in frequency between Bluetooth and IEEE 802.11b transmissions
- An advantage of the OLA schemes is that they do not require a centralized packet scheduler while the disadvantage is that they require changes to both the IEEE 802.11b standard and the Bluetooth specifications



BlueStar: An Integrated Solution to Bluetooth and 802.11

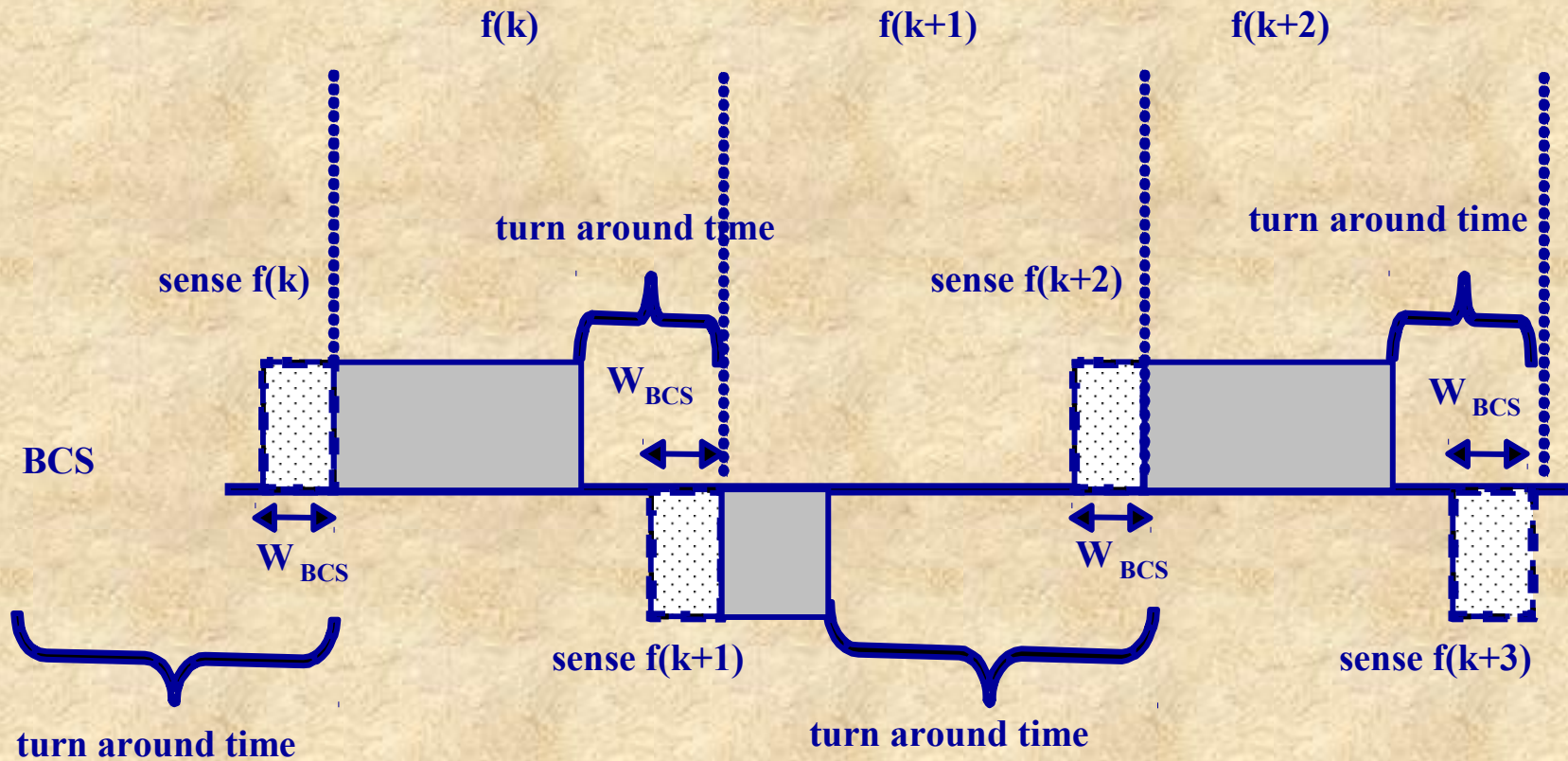
- As we have so far discussed, it is most likely that Bluetooth devices and IEEE 802.11 WLAN stations operating in the same 2.4 GHz ISM frequency band should be able to coexist as well as cooperate with each other, and access each other's resources
- These technologies are complementary to each other and such an integrated environment could be envisioned to allow Bluetooth devices to access the WLAN, and the Internet
- These cooperative requirements have lead to the BlueStar architecture, whereby few selected Bluetooth devices, called Bluetooth wireless gateways (BWG), are also members of a WLAN, thus empowering low-cost, short-range devices to access the global Internet infrastructure through the use of WLAN-based high-powered transmitters
- This architecture illustrated next

BlueStar Architecture



- To combat both intermittent and persistent interference and provide effective coexistence, a unique hybrid approach of **AFH** (adaptive frequency hopping) and a new mechanism called Bluetooth carrier sense (**BCS**) are employed in BlueStar
- AFH seeks to mitigate persistent interference by scanning the channels during a monitoring period and labeling them as “good” or “bad”, based on whether the packet error rate (PER) of the channel is below or above a given threshold
- BCS takes care of the intermittent interference by mandating that before any Bluetooth packet transmission, the transmitter has to sense the channel to determine the presence of any ongoing activity
- As shown in Figure 5.14 (on next slide), this channel sensing is performed during the turn around time of the current slot, and it does not require any changes to the current Bluetooth slot structure

Carrier Sensing Mechanism in Bluetooth





Intra Piconet Scheduling

- Bluetooth polling differs from classical polling in that the transmission from the master to a slave is always combined with the corresponding slave to master transmission
- Therefore, the master has only partial status knowledge of slaves' queue states, while it only knows its own queues
- Thus, classical polling models cannot be directly used, while they can still be used as benchmarks
- In case of an SCO link, the master has to poll the slave at regular intervals, given the stringent requirements of this type of traffic
- Therefore, for SCO links, the master device does not have much freedom to use one or another scheduling algorithm
- In case of an ACL link, however, polling can be performed in many different ways and so we focus only on scheduling for ACL links only



Intra & Inter Piconet Scheduling

The Limited and Weighted Round Robin Scheme (LWRR)

- **Limited and Weighted Round Robin (LWRR) adopts a weighted round robin algorithm with weights being dynamically changed according to the observed status of the queues**
- **In other words, LWRR considers the activeness of the slaves**
- **Initially, each slave is assigned a weight, say W , which is reduced by one each time a slave is polled and no data is exchanged**
- **Therefore, the slave misses as many chances in the polling cycle as is the difference between its current weight and W**
- **The lowest value that a slave's weight can achieve is one, meaning that it has to wait a maximum of $W-1$ cycles to send data**
- **Anytime there is a data exchange between the slave and the master, the weight of the slave is reset to the W value**



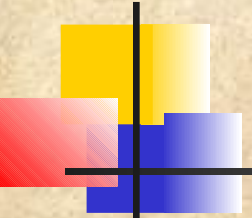
Intra & Inter Piconet Scheduling

- **The Pseudo-Random Cyclic Limited slot-Weighted Round Robin (PLsWRR) is based on two main properties:**
 - **It tries to distinguish between slaves on the basis of their “activeness”, i.e., according to the traffic history and PLsWRR reduces the rate of polling to less active slaves by not polling them for a certain number of slots (as opposed to cycles) which is the bounds for the maximum time between polls to a slave**
 - **The order in which slaves are polled in each cycle is determined in a pseudo-random manner so as to improve fairness and has been shown to provide a certain degree of fairness and perform well on scenarios with different traffic sources like TCP and CBR**
- **PLsWRR is comprised of two main parts: a Pseudo-Random Cycle of Polling and a Limited slot-weighted Round Robin (PLsWRR) scheme**



Fair Exhaustive Polling

- The Fair Exhaustive Polling (FEP) can be viewed as a combination of the strict round robin polling and the exhaustive polling
- The main idea is to poll slaves that probably have nothing to send
- FEP achieves this by introducing **two complementary states**, namely, the active state and the inactive state, and also by associating a weight with each slave
- In FEP, a polling cycle starts with the master moving all slaves to the active state, and then initiating one of the several possible polling sub cycles once in a round robin fashion
- One distinguish feature is that in FEP, the master performs the task of packet scheduling for both the downlink (master to slave) and uplink (slave to master) flows
- However, the master has only limited knowledge of the arrival processes at the slaves, which means that the scheduling of the uplink flows has to be based on the feedback it obtains when polling the slaves



Predictive Fair Poller

- The Predictive Fair Poller (PFP) is a polling scheme that takes both efficiency and fairness into account similar to LWRR and FEP
- For each slave, it predicts whether data is available or not and while at the same time keeping track of the fairness
- Based on these two aspects, it decides which slave to poll next and in the best effort case, PFP estimates the fair share of resources for each slave and keeps track of the fractions of these fair shares that each slave has been given
- PFP distinguishes two types of traffics: the best effort and the QoS-based
- For **best effort traffic**, PFP keeps track of both the fairness based on the fractions of fair share and the predictions, and thus can guarantee to poll the best effort traffic in a fair and efficient manner
- In the **QoS-based case**, QoS requirements are negotiated with the slaves and translated to fair QoS treatments and the polling unit, in turn, keeps track of the fractions of these fair QoS treatments that each slave has been given



Demand-Based Blooth Scheduling

- A flexible polling scheme is proposed that initially adopts common polling periods for all slaves, and subsequently increases the polling period for those slaves with less traffic load
- Similar to other schemes, the idea here is to poll slaves that probably have to send as little as possible
- Ultimately, the goal is to maximize throughput and to reduce the overall piconet power consumption
- This new polling scheme, referred to as Demand-Based Bluetooth Scheduling, is based on a scheduling table
- **Firstly**, the bridge nodes and the synchronous slaves are scheduled
- **Secondly**, the asynchronous dedicated slaves (ADSs) are scheduled



Inter Piconet Scheduling

Different inter-Piconet Scheduling schemes:

- ❑ *Distributed Scatternet Scheduling Algorithm (DSSA)*
- ❑ *Pseudo Random Scheduling Scheme (PCSS)*
- ❑ *Locally Coordinated Scheduling (LCS)*
- ❑ *Flexible Scatternet wide Scheduling (FSS)*
- ❑ *Credit Based Scheduling (CBS)*
- ❑ *The Load Adaptive Algorithm (LAA)*
- ❑ *The JUMP Mode Based Scheduling Algorithm*



Distributed Scatternet Scheduling Algorithm (DSSA)

- **Distributed Scatternet Scheduling Algorithm (DSSA) provides a conflict free access to the shared medium**
- **DSSA is based on the assumption that nodes have distinct identities (IDs) and are aware of the identities and traffic requirements of their neighbors**
- **In DSSA, each master needs the permission of all its neighbors to schedule its piconet**
- **Permission is granted to the neighboring master with the highest ID among those neighboring masters that have not yet scheduled their piconets**
- **DSSA is an ideal algorithm as it assumes that nodes are aware of the traffic requirements of their neighbors, which cannot be realized in a real scenario**
- **In addition, given the requirement that the solution is carried out from the highest ID master to lowest ID master, not all master devices are treated equally**



Pseudo Random Scheduling Scheme

(PCSS)

- Different from the hard scheme of DSSA, the Pseudo Random Scheduling Scheme (PCSS) falls in the category of soft coordination schemes, wherein the nodes decide their presence in piconets based on local information
- By nature, soft coordination schemes cannot guarantee conflict-free participation of bridge nodes in different piconets; however, they will have much lower complexity than hard coordination schemes
- In the PCSS algorithm, coordination is achieved by implicit rules in the communication without the need of exchanging explicit control information
- The low complexity of the algorithm and its conformance to the current Bluetooth specification makes it easy to be incorporated
- Every node randomly chooses a communication checkpoint that is computed based on the master's clock and the slave's device address



Locally Coordinated Scheduling

(LCS)

- While there are conflicts in the PCSS scheme, the Locally Coordinated Scheduling (LCS) scheme coordinates nodes in a manner that eliminates all scheduling conflicts
- In response to bursty traffic on a link, LCS adjusts both the intervals between communication events and the duration of those events, while PCSS changes only the intervals between communication events
- LCS is based on the concept of scheduled meetings called appointments and optimizes the overall efficiency of the scatternet in terms of throughput, latency and energy, by minimizing wasted and missed communication opportunities
- It also allows nodes to tradeoff between energy efficiency and latency
- However, LCS can only be applied to loop-free scatternet topologies and LCS achieves high TCP throughput, low packet latency and low node activity time (which corresponds to low energy consumption) for low bandwidth applications



Flexible Scatternet wide Scheduling *(FSS)*

- FSS consists of two algorithms: a flexible traffic scheduling algorithm executed by each master, and an adaptive switch-table modification algorithm executed by each bridge node
- FSS is based on a switch-table concept, which is constructed when the scatternet is formed
- Each bridge node uses a switch-table to direct switch between its multiple piconets
- To avoid bridge conflicts, a master polls a bridge node only at those slots when the bridge node is known to be synchronized to the piconet controlled by the master
- Each master, in turn, employs a flexible traffic scheduling algorithm to schedules both dedicated slaves and bridge nodes
- Moreover, the switch-table can be dynamically adjusted based on the traffic load so as to improve the system performance
- Compared to some static schemes, FSS can significantly improve the system throughput and reduce the packet transmission delay



Credit Based Scheduling (CBS)

- The CBS algorithm is based on the Bluetooth sniff mode that defines presence points for each inter-piconet link at which communication may start
- The rationale behind these presence points, is to enable each device to quickly determine whether the peer device is in the same piconet
- If so, the communication may start between the devices, otherwise another presence point may be tried without having lost much bandwidth
- The length of a particular communication period is not predetermined, as it depends on the current link utilization and the amount of data to be exchanged
- Interestingly, the presence points and the dynamic length of communication periods may be mapped directly onto the sniff mode, requiring little or no changes to the current Bluetooth specification
- The communication schedule is then determined online for each communication period



Intra & Inter Piconet Scheduling

The Load Adaptive Algorithm (LAA)

- **While CBS uses the sniff mode, LAA uses the hold mode**
- **The primary difference between these two modes is that the duration of the hold period is set every time the slave is placed in the hold mode, whereas the parameters of the sniff mode are set once and can be reused for many intervals**
- **Thus, the hold mode requires repeated negotiations that waste at least a pair of slots, while the sniff mode requires a single negotiation**
- **Therefore, the sniff mode may be more suitable for steady traffic, whereas bursty traffic may be better supported by the hold mode**
- **LAA manages the scheduling mechanism of the bridge by determining the duration of the bridge activity in the different piconets, so that the delay incurred by packets requiring inter-piconet routing can be reduced**
- **The algorithm adapts to varying loads by utilizing information regarding its queues to the different masters, and also by using information transferred by the masters**



Jump Mode Based Scheduling Algorithm

- This mode includes a set of communication rules that enable efficient scatternet operation by offering a great deal of flexibility for a node to adapt its activity in different piconets to the traffic conditions
- Using the JUMP mode, a bridge node divides the time into *time windows* and then signals about which piconet it is going to be present for each of these time windows
- The time windows are of pseudo random length to eliminate systematic collisions and thereby avoid starvation and live-lock problems without any need for scatternet-wide coordination
- Besides enabling scatternet operation, the JUMP mode may also enhance other aspects of Bluetooth such as the low-power operation
- Table 5.4 compares various scatternet scheduling algorithms discussed so far




Comparison of Scatternet Scheduling Algorithms

	DSSA	PCSS	LCS	FSS	LAA	CBS	JUMP mode
Dynamic	No	Yes	Yes	Yes	Yes	Yes	Yes
Ideal	Yes	No	No	No	No	No	No
QoS	No	No	No	Yes	No	Yes	No
Scatternet topology	Any	Any	Loop-free	Any	Any	Any	Any
Modifies Bluetooth specification	No	No	Yes	No	No	No	Yes
Computational complexity	High	Low	High	Quite low	Low	Low	Low
Feasibility	No	No	No	Yes	Yes	Yes	No
Basic Technique	Graph theory	Pseudo random technique	Appointment	Switch table	Hold mode	Credit scheme	JUMP mode



Selecting Bridge

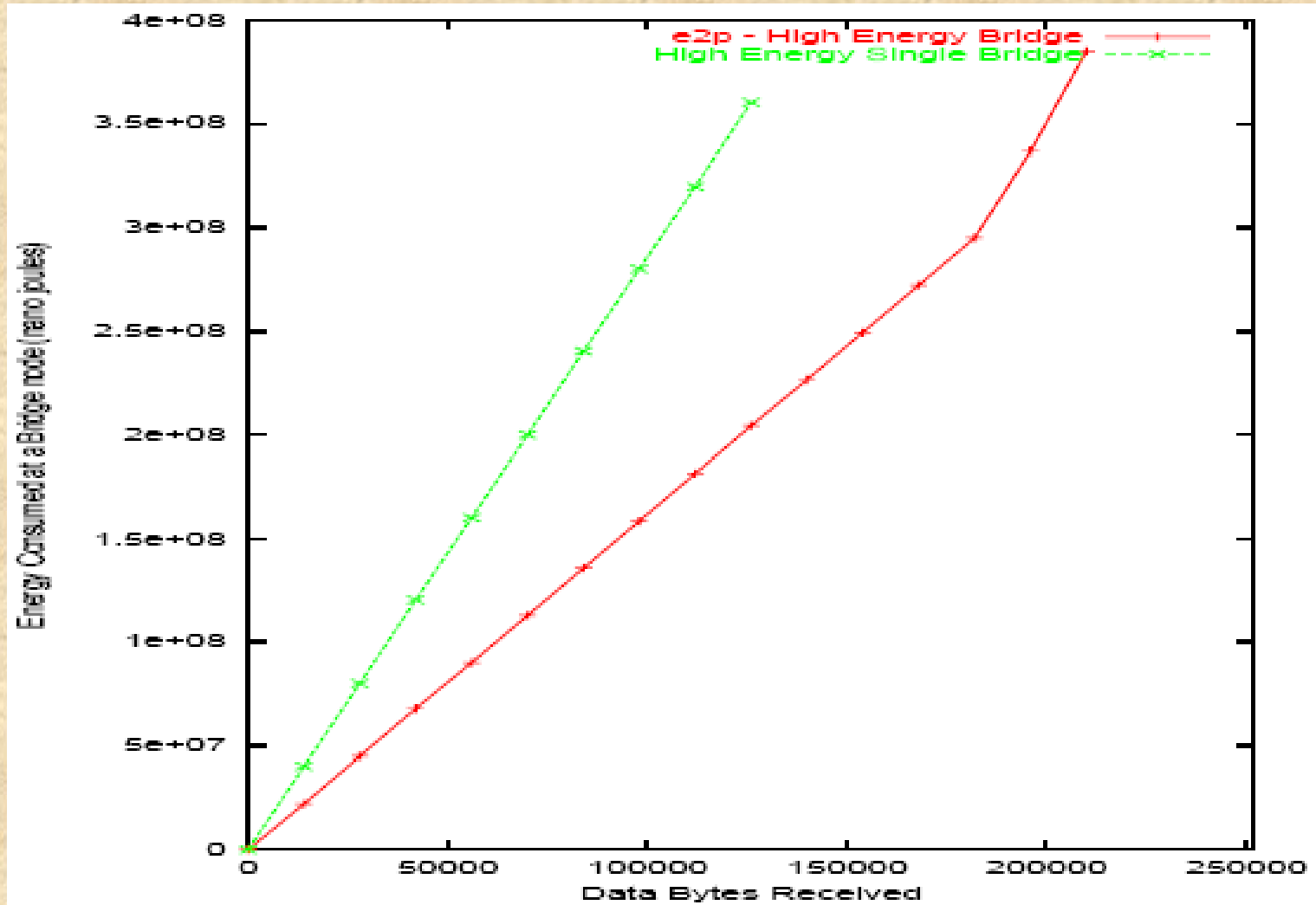
- In Bluetooth large ad hoc networks are formed by inter-linking individual piconets to form a scatternet
- Scatternets are formed by sharing one or more slaves (the bridges nodes) in a time division multiplexed system, wherein the bridges share their active time period between two piconets
- Theoretically, the **bridge can be a master in one piconet and a slave in another piconet**, or a slave in both piconets
- In practice, however, most current research considers bridges in the slave-slave configuration only, as having a bridge to be a master in one piconet will result in this piconet being idle every time the bridge is in some other piconet
- The bridge bears the responsibility of a switch, buffering incoming data packets, then switching to another piconet and relaying the buffered packets to a new master
- This means that they are always transmitting, receiving or switching between piconets



Selecting Bridge: Energy Efficient Protocol

- The first scheme is a simple Energy Efficient Protocol (E2P), in which the master decides on a set of nodes that are designated as prospective bridges
- The master then chooses **two nodes** to function as bridges
- These nodes are typically the best in terms of computing and energy resources
- The master then tries to distribute the traffic among the two, sending packets to the two bridges in a round robin fashion (other scheduling algorithms could also be employed)
- The bridges buffer the incoming data packets, and then switch at the same time for a pre-defined SNIFF period previously agreed upon by the masters of both piconets, through any bridge negotiation protocol
- This simple division seems to work well, improving energy savings by about 43% as shown in Figure 5.13

Energy Consumption (Single Bridge V/s $E2P$)

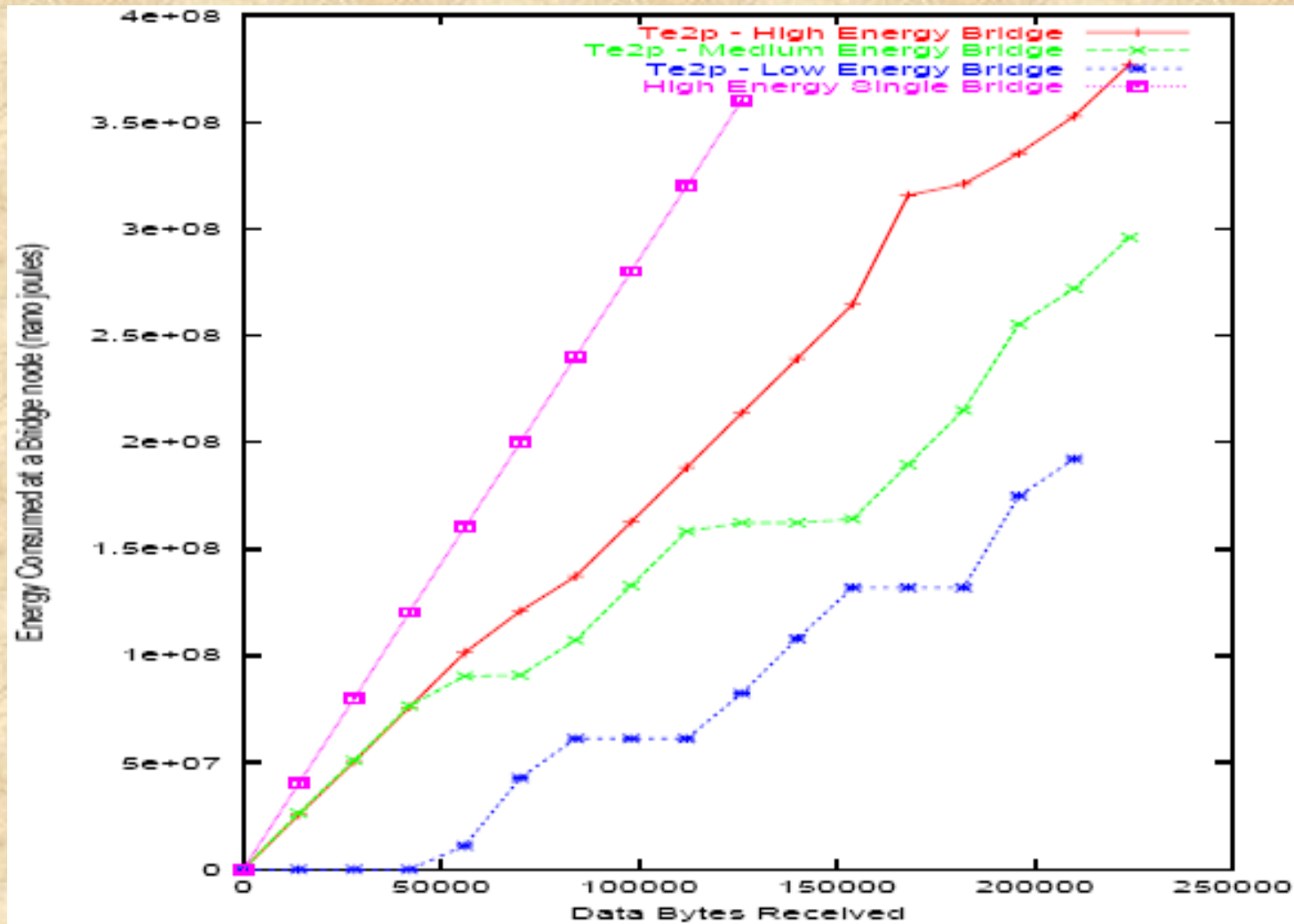




Threshold-based Energy Efficient Protocol (TE2P)

- The second approach, TE2P dynamically select bridges and change the bridges based on their energy settings
- Every device calculates and sets its own Soft Threshold (ST) and Hard Threshold (HT)
- The ST defines a value at which the node would *prefer* to share its load with another node but can still work alone (like say 70% of total power available), while the HT defines a *critical* value where the node definitely needs to share its load (for example, 30% of the total power)
- These values are then passed on to the master of the piconet
- The ST and HT values may vary for different devices due to varying hardware and software configurations
- The master chooses a set of prospective bridges (B) based on their energy and traffic requirements and the traffic is then divided among the bridges

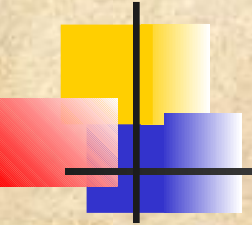
Energy consumption pattern in TE2P





Traffic Engineering

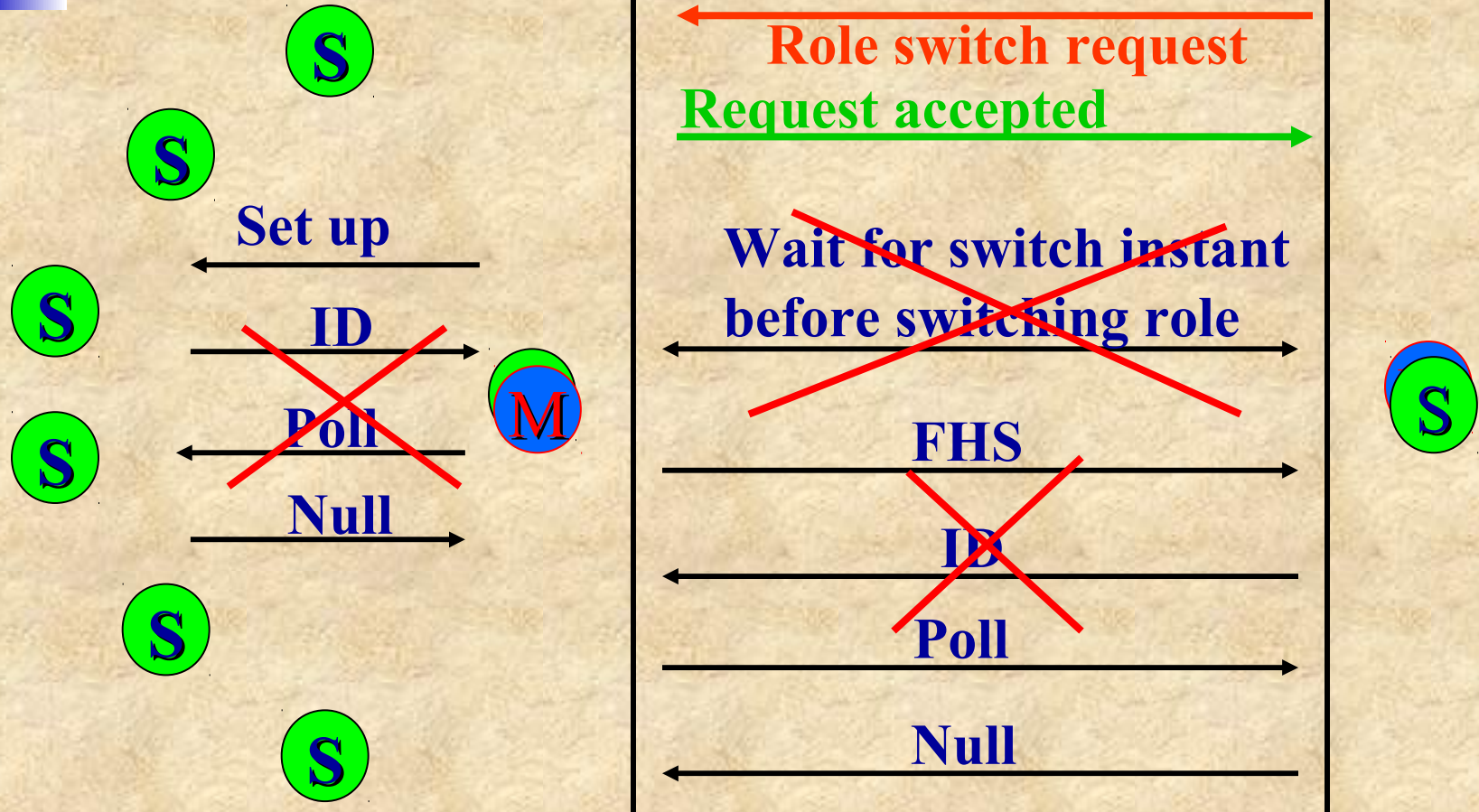
- If a larger number of connections ought to be supported, it either drastically increases the delay or simply blocks the incoming traffic
- The bottom line of these problems is the **lack** of Traffic Engineering techniques in current Bluetooth
- Traffic Engineering has been shown to be extremely useful for Internet, by efficiently transferring information from a source to an arbitrary destination with controlled routing function that steer traffic through the network
- A systematic application of Traffic Engineering helps in enhancing the QoS delivered to end-users, and aids in analyzing these results
- Traffic Engineering suggests both demand side and supply side policies for minimizing congestion and improving QoS
- Demand side policies restrict access to congested resources, dynamically regulates the demand to alleviate the overloaded condition, or control the way the data is routed in the network
- Supply side policies augment network capacity to better accommodate the traffic



Pseudo Role Switch (PRS)

- PRS would not require any change in FHS as this scheme keeps the piconet synchronized on the previous piconet parameters
- Demand side traffic engineering are suggested by categorizing the requests based on the type of data being transmitted
- For example, Audio data has critical latency requirements, Telnet traffic needs quick response time, FTP traffic needs reliable communication, etc. and priority is given to those connections which have stringent QoS requirements while at the same time supporting less constrained communications
- Figure 5.15(a) shows the graph for data bytes received versus actual information transmitted over the network where FTP connection is followed by Telnet connection and Telnet is followed by SCO connection
- Moreover, the delay characteristics in Figure 5.15(b) reveals that this PRS scheme manages to reduce the delay to almost $\frac{1}{2}$ of its original value

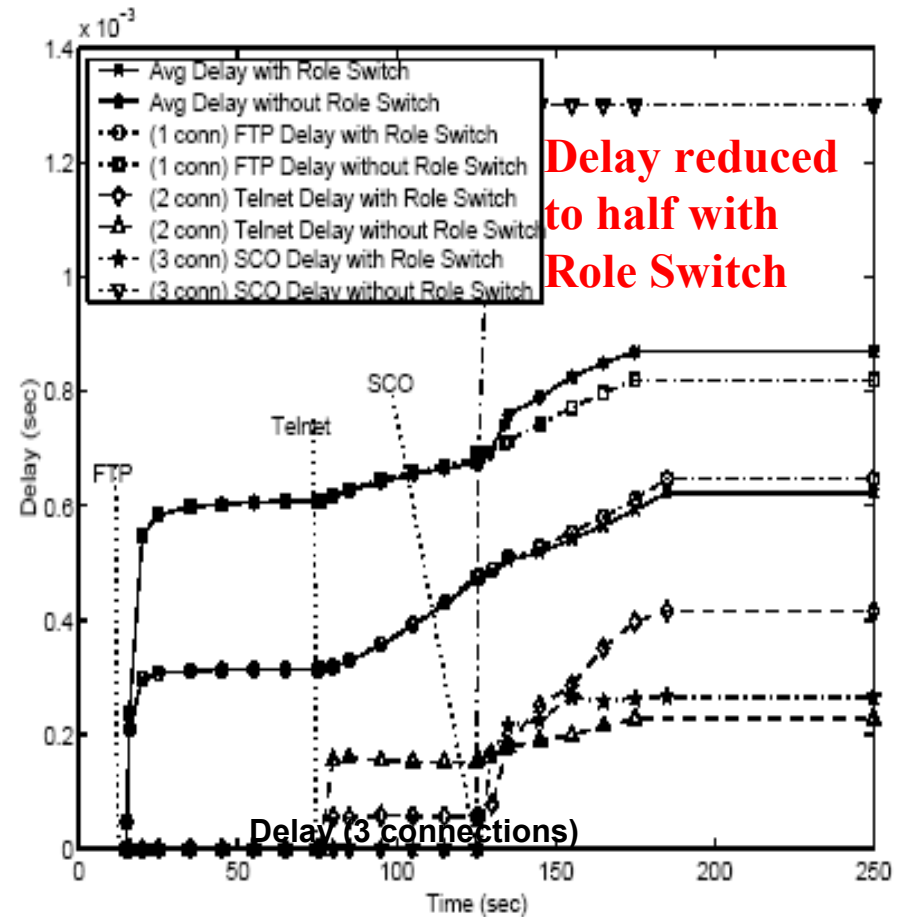
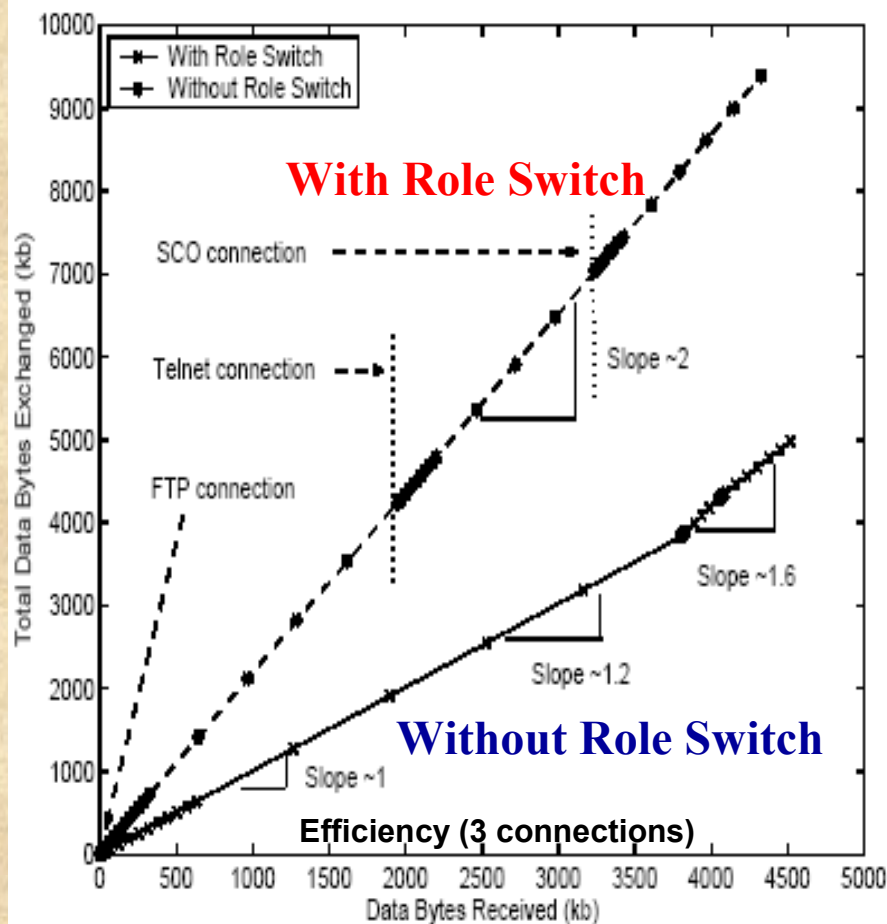
Pseudo Role Switching of the Master



Master-Slave Switch

**Time consuming step avoided by Pseudo Role Switching
and achieve substantial throughput improvement**

Data Bytes Received v/s Actual Information Transmitted and Delay



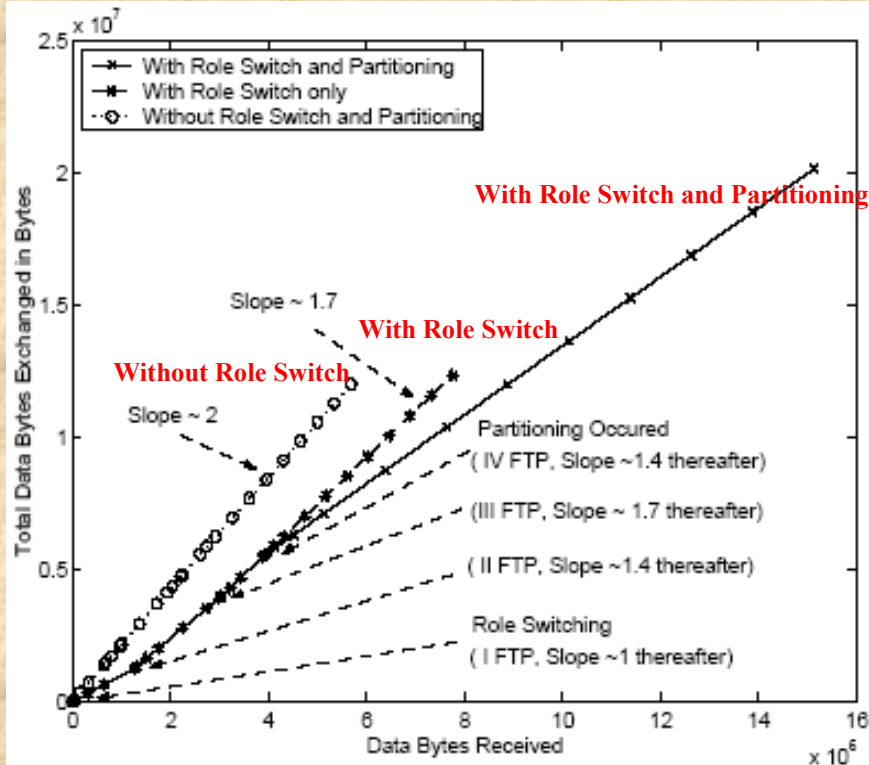


Pseudo Partitioning

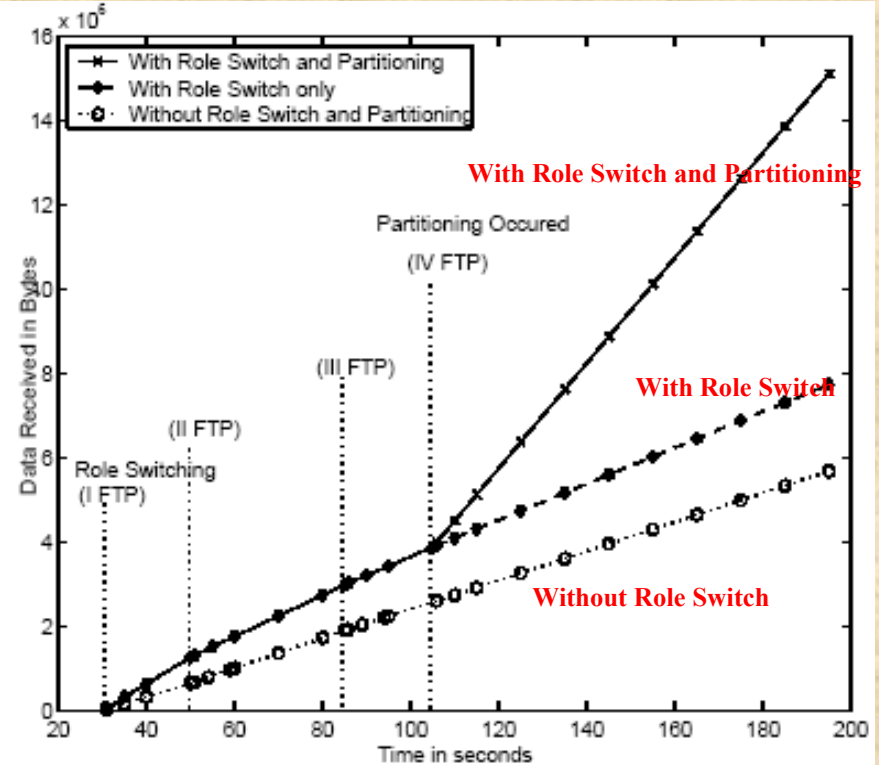
- In PPR, the piconet is **partitioned** when the need for bandwidth cannot be fulfilled by the current structure
- The decision partitions the piconet in such a way that devices, which are consuming most of the bandwidth and does not involve the current master, are separated
- Also, this type of partitioning should not last forever and rejoining the piconet should be made possible as soon as the traffic in one of the piconet ends
- Certain threshold value should be maintained to avoid continuous partitioning and rejoining upon every connection arrival and termination
- Such a decision can only be taken if the master knows negotiated QoS parameters while establishing all previous connections
- The performance of PPR under overloaded conditions by dynamically generating FTP connection requests has been evaluated

4 FTP connections: Efficiency and Throughput

- Number of total packets transmitted per data packet received ratio is minimized when both PRS and PPR schemes are in action, as depicted in Figures 5.16(a)
- Increased aggregate throughput: Figure 5.16(b) shows that the improved performance of PPR



Efficiency (4 FTP connections)



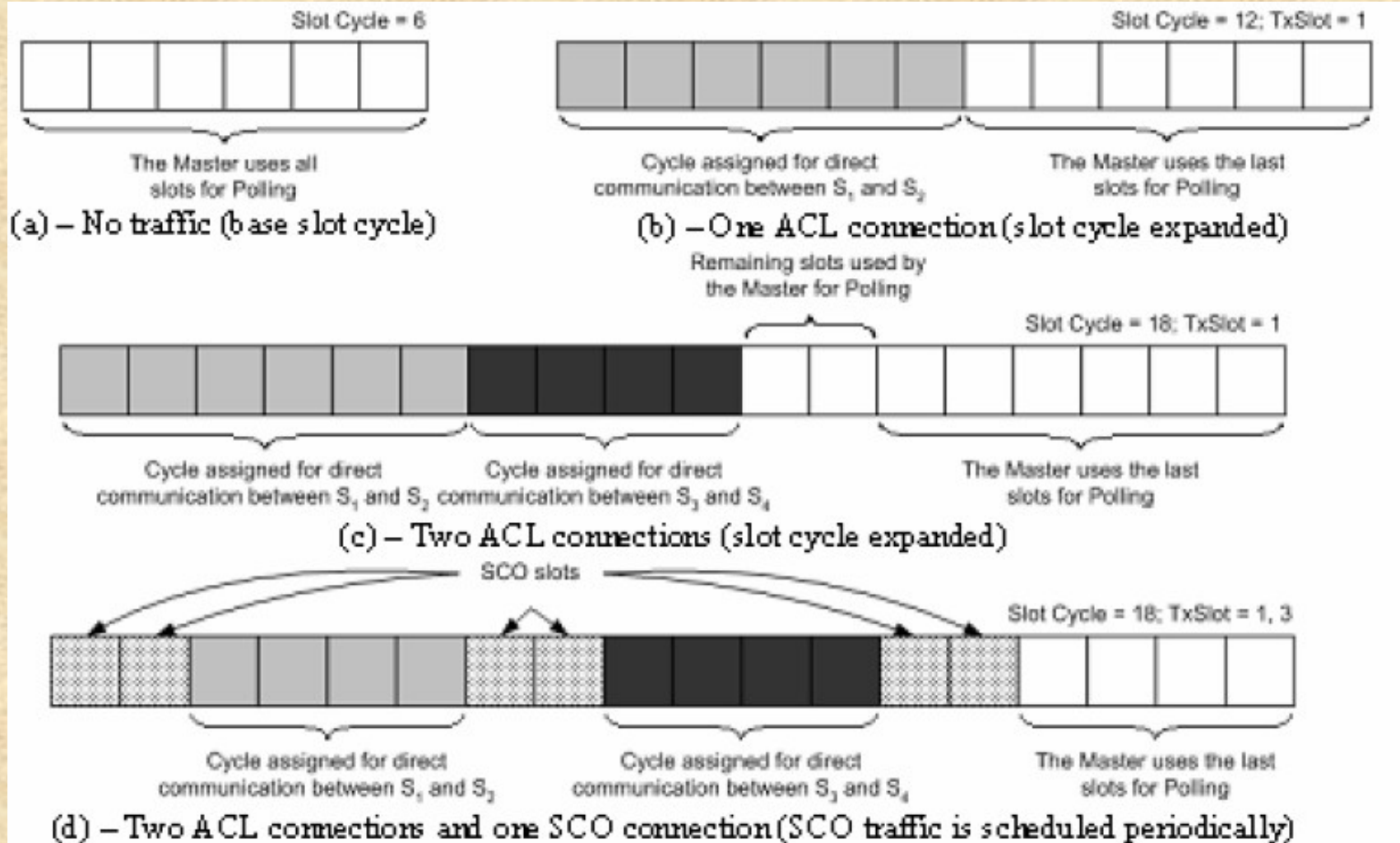
Throughput (4 FTP connections)

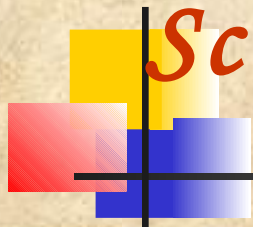


QoS and Dynamic Slot Assignment

- A novel QoS-driven Enhanced Dynamic Slot Assignment (EDSA) scheme has been proposed to address major shortcomings in the Bluetooth design while keeping the simplicity of the Master/Slave paradigm
- The basic strategy is to combine the QoS-driven Dynamic Slot Assignment (DSA) and the dynamic piconet partitioning
- Here, DSA-only is employed at the piconet level while dynamic partitioning opens up the scope of DSA to the scatternet level
- The basic idea behind DSA is to appropriately manage the polling cycle conducted by the master of the piconet, given the connection QoS requirements
- As shown in Figure 5.17, as devices initiate or terminate communication with each other within the piconet, the piconet polling cycle is restructured, a new transmission schedule is built for each piconet device, and then the resulting schedule is propagated to the members of the piconet

Dynamic Assignment of Slots






Scatternet Formation

- Scatternet formation algorithm denominated as Bluetooth Topology Construction Protocol (BTCP) has three phases:
 - ▣ A coordinator is elected with a complete knowledge of all devices
 - ▣ This coordinator determines and tells other masters how a scatternet should be formed
 - ▣ The scatternet is formed according to these instructions
- Since the topology is decided by a single device (the coordinator), BTCP has more flexibility in constructing the scatternet
- However, if the coordinator fails, the formation protocol has to be restarted
- BTCP's timeout value for the first phase would affect the probability that a scatternet is formed
- In addition, BTCP is not suitable for dynamic environments where devices can join and leave after the scatternet is formed

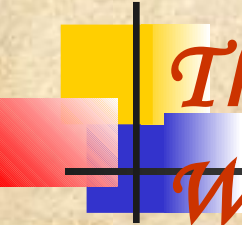
▪ **See: UCBT–Bluetooth Simulator for ns-2 (www.eecs.uc.edu/~cdmc/UCBT?)**



The IEEE 802.15 Working Group for WPANs

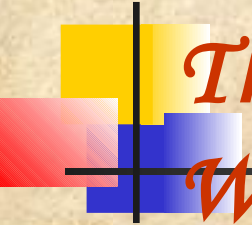
A single WPAN is intended to be a network in the home or office with no more than 8 to 16 nodes and altogether, 802.15 WG is formed by five TGs:

- IEEE 802.15 WPAN/Bluetooth TG 1 (802.15.1) – The TG 1 was established to support applications which require medium-rate WPANs (such as Bluetooth); these WPANs handles a variety of tasks ranging from cell phones to PDA communications, have a QoS suitable for voice applications and this TG is derived a Wireless Personal Area Network standard based on the Bluetooth v1.1 specifications**
- IEEE 802.15 Coexistence TG 2 (802.15.2) – Several wireless standards, such as Bluetooth and IEEE 802.11b, and appliances, such as microwaves and cordless phones, operate in the unlicensed 2.4 GHz ISM frequency band and the TG 2 has developed recommended practices to facilitate collocated operation of WPANs and WLANs to promote better coexistence of IEEE 802 wireless technologies,**



The IEEE 802.15 Working Group for WPANs

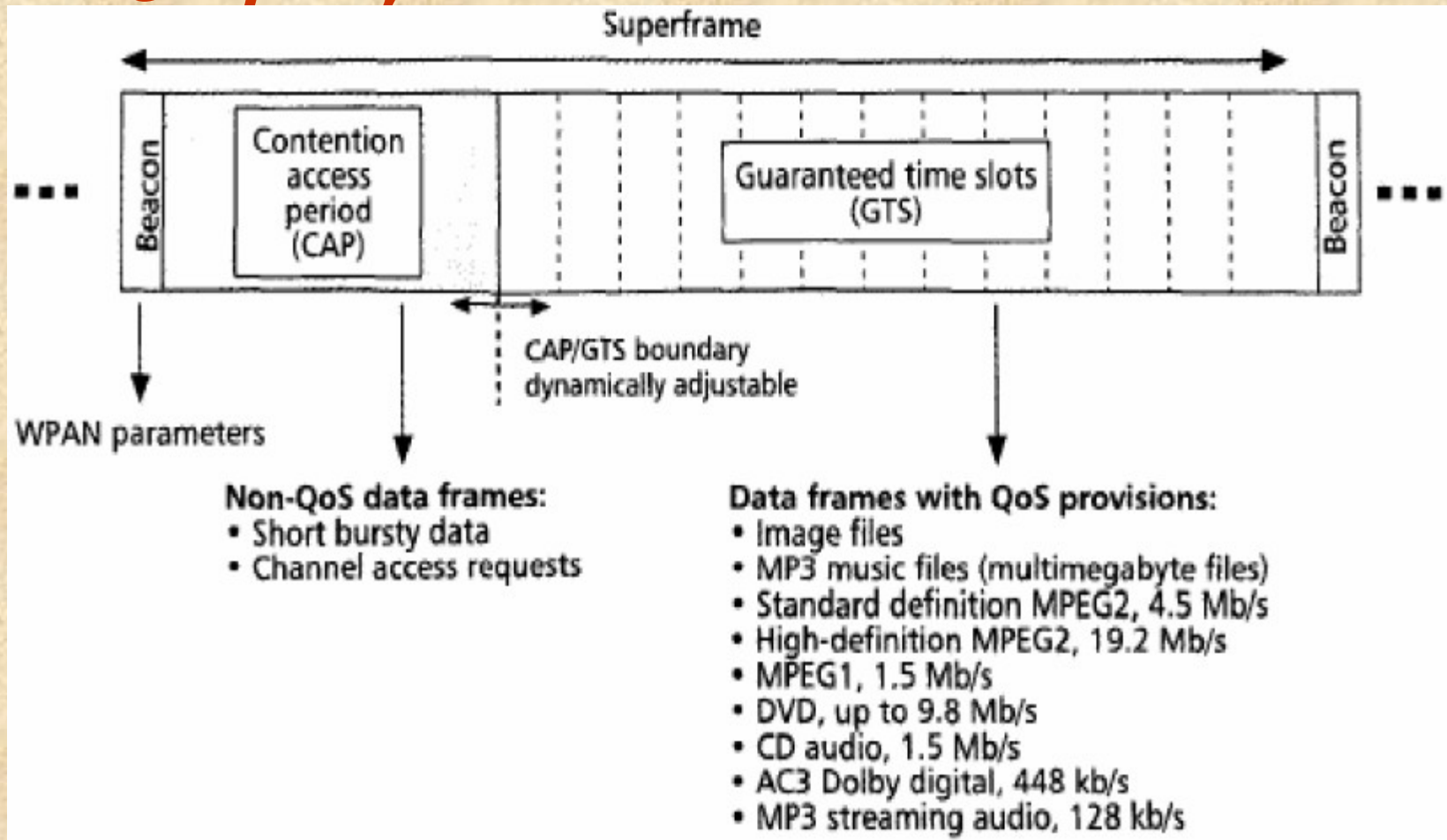
- ❑ **IEEE 802.15 WPAN/High Rate TG 3 (802.15.3)** – The TG 3 for WPANs has defined standards for high-rate (from 55 Mbps up to 480 Mbps) WPANs and besides a high data rate, this standard provides for low power, low cost solutions addressing the needs of portable consumer digital imaging and multimedia applications
- ❑ **IEEE 802.15 WPAN/Low Rate TG 4 (802.15.4)** – The TG 4 has defined a standard having ultra-low complexity, cost, and power for a low-data-rate (200 Kbps or less) wireless connectivity among fixed, portable, and moving devices as location awareness is considered as a unique capability of the standard, potential applications include sensors, interactive toys, smart badges, remote controls, and home automation
- ❑ **IEEE 802.15 WPAN/Mesh TG 5 (802.15.5)** – The TG 5 is chartered to determine the necessary mechanisms that must be present in the PHY and MAC layers of WPANs to enable mesh networking which is a PAN that employs one of two connection arrangements: full mesh topology or partial mesh topology

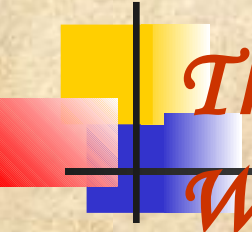


The IEEE 802.15 Working Group for WPANs

- The 802.15.3 MAC layer specification is designed from the ground up to support ad hoc networking, multimedia QoS provisioning, and power management
- In an ad hoc network, devices can assume either master or slave functionality based on existing network conditions
- Devices in an ad hoc network can join or leave an existing network without complicated setup procedures
- Figure 5.18 illustrates the MAC superframe structure that consists of a network beacon interval, a contention access period (CAP) and guaranteed time slots (GTS)
- The boundary between the CAP and GTS periods is dynamically adjustable
- A network beacon is transmitted at the beginning of each superframe, carrying WPAN-specific parameters, including power management, and information for new devices to join the ad hoc network

IEEE 802.15.3 MAC Superframe





The IEEE 802.15 Working Group for WPANs

- On the surface, 802.15.3 could be seen as a source of competition to Bluetooth, and in reality this is not the case
- Admittedly, the concept of 802.15.3 is to allow for a chipset solution that would eventually be approximately 50% more expensive than a Bluetooth solution
- Furthermore, the power consumption and size would be about 50% greater than a Bluetooth solution
- However, on the flip-side 802.15.3 would allow for data rates considerably in excess of current sub-1 Mbps Bluetooth solutions and is a critical differentiating element
- In effect, 802.15.3 is being positioned to be a complementary WPAN solution to Bluetooth
- This is particularly the case since the Bluetooth SIG is going slowly on its efforts to develop the next-generation Bluetooth Radio 2, which would allow for data rates between 2 Mbps and 10 Mbps



IEEE 802.15.3 Working Group for WPANs

- Some view that there is actually more potential for 802.15.3 to be seen as overlapping with 802.11-based protocols than with Bluetooth
- With 802.11-based wireless LANs pushing 54 Mbps and the work being done by the 802.11e TG on the QoS support, it is clear that wireless LANs are also looking to become a serious contender for multimedia applications
- Even though 802.15.3 is being designed from scratch and would theoretically offer superior bandwidth for multimedia applications at favorable cost and power consumption metrics, it will be difficult to distinguish itself from full-fledged 802.11-based wireless LANs
- Even so, one source of difference is that 802.15.3 is meant to be optimized for PAN distances while WLAN range is clearly larger



IEEE 802.15.4 Working Group for WPANs

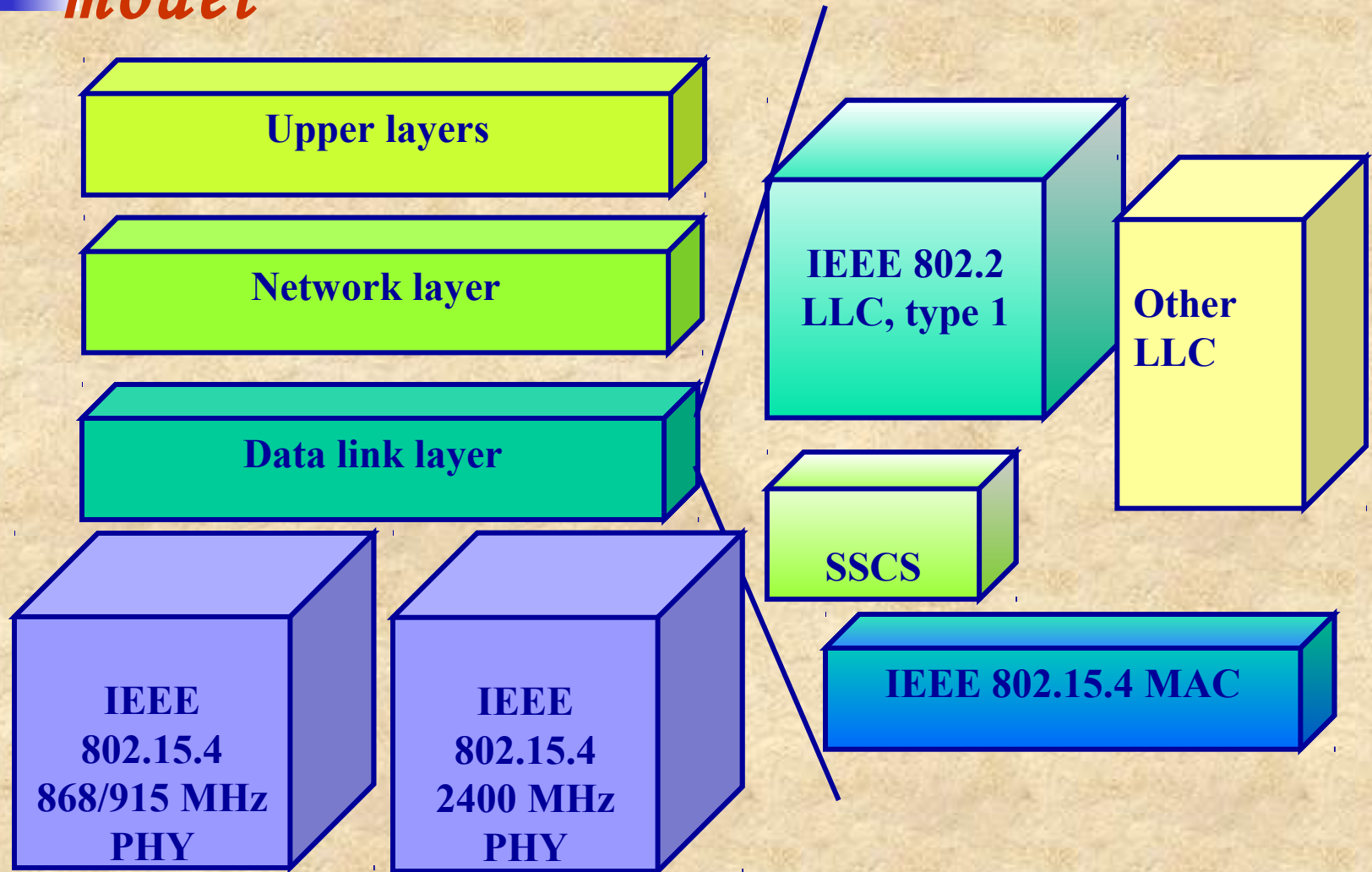
- IEEE 802.15.4 defines a specification for low-rate, low-power wireless personal area networks **(LR-WPAN)**
- It is extremely well suited to those home networking applications where the key motivations are reduced installation cost and low power consumption
- There are some applications that require high data rates like shared Internet access, distributed home entertainment and networked gaming
- However, there is an even bigger market for home automation, security and energy conservation applications, which typically do not require the high bandwidths associated with the former category of applications
- Application areas include industrial control, agricultural, vehicular and medical sensors and actuators that have relaxed data rate requirements



IEEE 802.15.4 Working Group for WPANs

- The Data Link Layer (DLL) is split into two sublayers – the MAC and the Logical Link Control (LLC)
- The LLC is standardized in the 802 family while the MAC varies depending on the hardware requirements
- Figure 5.19 shows the correspondence of the 802.15.4 to the ISO-OSI reference model
- The IEEE 802.15.4 MAC provides services to an IEEE 802.2 type I LLC through the Service Specific Convergence Sub layer (SSCS)
- A proprietary LLC can access the MAC layer directly without going through the SSCS
- The SSCS ensures compatibility between different LLC sub layers and allows the MAC to be accessed through a single set of access points

802.15.4 in the ISO-OSI layered network model

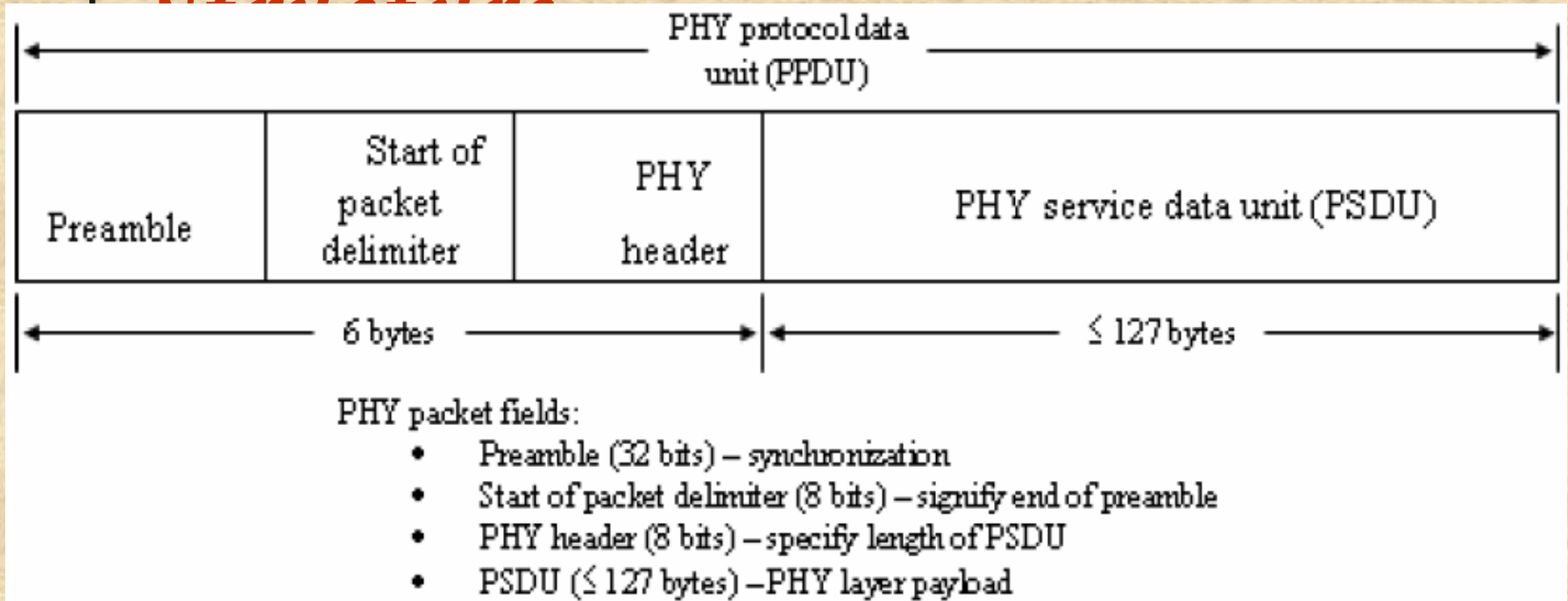




IEEE 802.15.4 Working Group for WPANs

- IEEE 802.15.4 offers two PHY layer choices based on the DSSS technique and share the same basic packet structure for low duty cycle low power operation
- The difference lies in the frequency band of operation: one specification is for the 2.4 GHz ISM band available worldwide and the other is for the 868/915 MHz for Europe and USA, respectively
- These offer an alternative to the growing congestion in the ISM band due to a large-scale proliferation of devices like microwave ovens, etc. and also differ with respect to the data rates supported
- The ISM band PHY layer offers a transmission rate of 250 kbps while the 868/915 MHz offers 20 and 40 kbps
- The lower rate can be translated into better sensitivity and larger coverage area, while the higher rate of the 2.4 GHz band can be used to attain lower duty cycle, higher throughput and lower latencies

802.15.4 PHY Layer Packet



- The two PHY layers though different, maintain a common interface to the MAC layer, i.e., they share a single packet structure as shown
- The packet or PHY protocol data unit (PPDU) consists of the synchronization header, a PHY header for the packet length, and the payload itself which is also referred to as the PHY service data unit (PSDU)



Comparison between WPAN Systems

To understand the suitability of these systems for WPAN applications, there are several criteria keeping in mind the overall goal of forming ad hoc networks using simple, low power, small, cost effective devices. They are:

- ❑ **Range:** The communication range of the device
- ❑ **Data Rate:** The maximum data rate possible in the network
- ❑ **Support for Voice:** Support a protocol or method to allow voice communication
- ❑ **Power Management:** A true method for devices to conserve power
- ❑ **LAN Integration:** A method to integrate the WPAN with a standard LAN such as Ethernet or 802.11



Comparison between WPAN Systems

- WPAN computing will typically involve communication with devices within a few meters
- Ten meters is usually considered sufficient for these devices to collaborate and provide services, like an ad hoc network for meetings in small rooms, study sessions in libraries, or home networking for computers or consumer devices
- This distance allows devices to have some flexibility in terms of how close they are
- Bluetooth can support up to 10 meters and when external power sources are utilized, **100-meter range** can be achieved
- IEEE 802.15.3 can also support a 10 meter range while 802.15.4 can support 10-20 meters depending on the sensitivity of the receiver
- Bluetooth and IEEE 802.15.3 support at least a 10-meter range, with the ability to pass through minor obstructions



Comparison between WPAN Systems

- Data rate is an application driven requirement
- WPAN technologies cover all kinds of data rates, from a very low data rate to transmit text between two devices to a high data rate for Internet access
- The concept of a WPAN is relatively new and applications for the technology have not matured enough to push the limits of the available data rates
- Bluetooth allows for up to eight devices to operate in a single piconet and transmit data in symmetric (up to 432.6 kbps) or asymmetric (up to 721 kbps and 57.6 kbps) mode
- The 802.15.3 is able to provide data rates ranging from **11 Mbps to 55 Mbps**
- For the applications available today, this may be considered more than sufficient as IEEE 802.15.4, seems ideal only for the LR-WPAN providing services of 20-250 kbps (e.g., wireless sensor networks)



Comparison between WPAN Systems

- A WPAN technology is most likely to be embedded into existing devices such as mobile phones, PDAs and pagers, and hence voice communication as well as integration with the PSTN is highly desirable
- Bluetooth's voice support is provided by the Telephony Control protocol Specification (TCS) Binary, which is based on ITU-T Recommendation Q.931 for voice
- Bluetooth matches standard telephony with a 64 kbps data rate and can support calls for all eight members of a piconet
- In a Bluetooth WPAN, a single Bluetooth enabled voice device (mobile phone) can act as a gateway for all other devices
- IEEE 802.15.3 with its GTS can support all kinds of multimedia traffic from simple image files to high definition MPEG-2 at 19.2 Mbps and MP3 streaming audio at 128 kbps
- On the other hand, IEEE 802.15.4 was never designed to support voice, though there are mechanisms for time-bounded data services within the context of an LR-WPAN



Support for LAN Integration

- **The ability to communicate with a LAN allows WPAN devices to take advantage of services such as printing, Internet access and file sharing**
- **Bluetooth has a profile that allows LAN access using the Point-to-Point Protocol (PPP) over RFCOMM**
- **It does not provide LAN emulation or other methods of LAN access, just the features that are standard in PPP such as compression, encryption, authentication and multi-protocol encapsulation**
- **To access LAN services, a Bluetooth-enabled LAN device which has access to LAN media like Ethernet, 802.11, etc., is needed**
- **The IEEE 802.15.3 forms ad hoc networks using the concept of master and slave roles, and supports LAN integration in a way similar to Bluetooth**



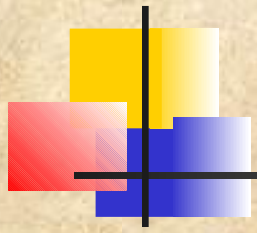
Power Management

- Bluetooth has a standby and peak power range of less than **1 mA to 60 mA** and allows devices to enter low power states without losing connectivity to the WPAN piconet
- It has three low power states – PARK, HOLD, and SNIFF and a normal power state when the device is transmitting while the power savings varies due to the reduced transmit-receive duty cycle
- The IEEE 802.15.3 standard has advanced power management features with a current drain of just **80 mA** while actively transmitting and very minimal when in power save mode
- It also is able to support QoS functionality, even when it is in a power save mode
- It has three modes of power management – the Piconet Synchronized Power Save (PSPS) mode, the Synchronized Power Save (SPS) mode and the Hibernate mode and has been designed ground-up for low power operation, in some cases stretching the battery life for several years



Comparison between WPAN Systems

- Based on the above analysis, it seems that the front runners for WPANs are Bluetooth, IEEE 802.15.3 and IEEE 802.15.4. These three broadly meet the standard criteria of size, cost, simplicity, and low power consumption
- IEEE 802.15.3 definitely has the upper edge since it can offer much higher data rates, good power control, extremely low connection setup times, advanced security features (see Table 5.5) and a plethora of QoS services for high end multimedia traffic even under low power operation
- In the context of WPAN computing today, it is sometimes seen as an excess of everything, whereas Bluetooth may to a large extent cover WPAN computing needs in the short-term future
- IEEE 802.15.4, on the other hand, is extremely suitable for very low power applications such as sensor networking and home automation, something that Bluetooth and IEEE 802.15.3 are clearly not meant for and Table 5.5 provides a comparison of the various WPAN systems discussed so far



Comparison of various WPANs

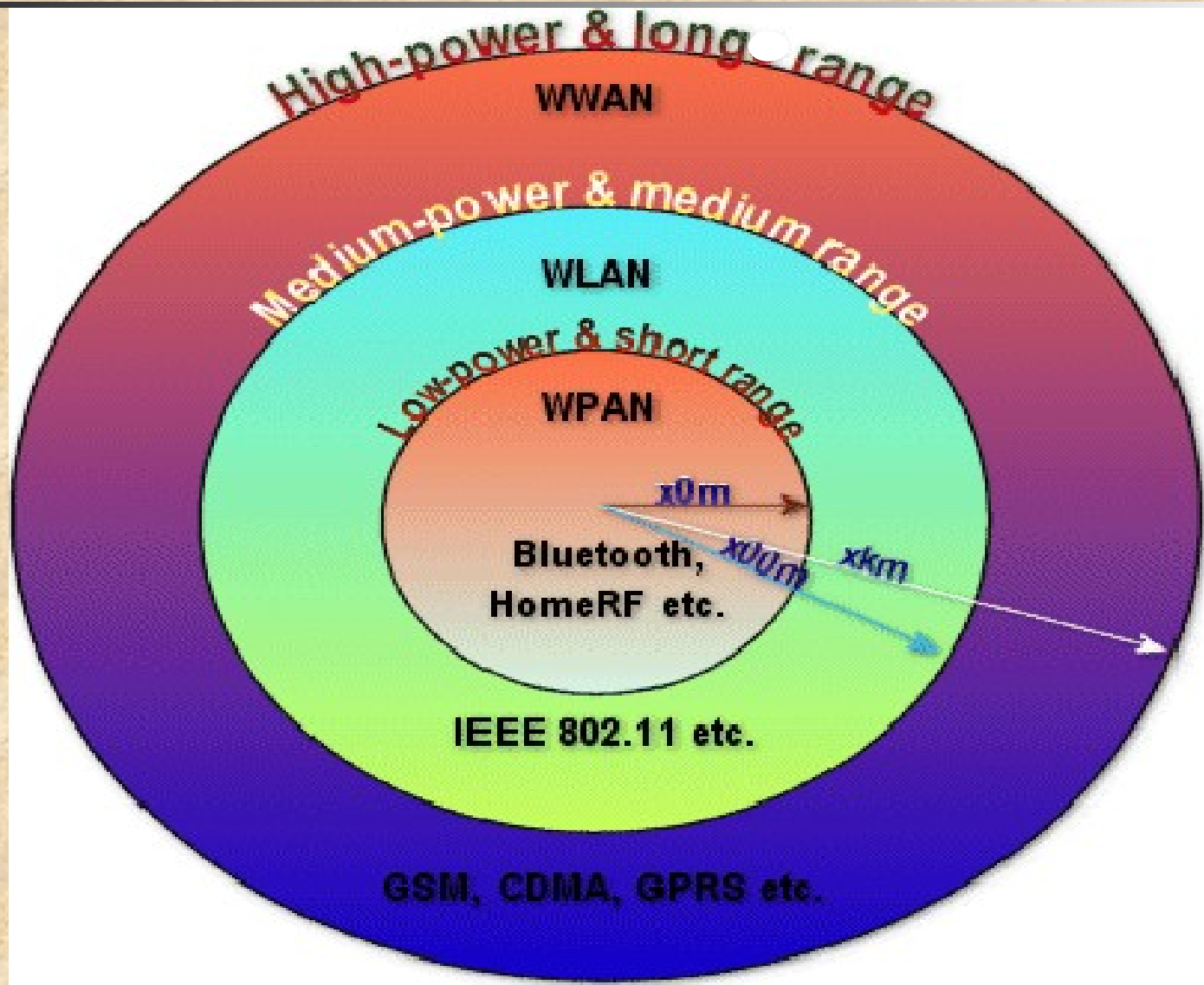
Technology	Bluetooth (IEEE 802.15.1)	IEEE 802.15.3	IEEE 802.15.4
Operational Spectrum	2.4 GHz ISM band	2.402 – 2.480 GHz ISM band	2.4 GHz and 868/915 MHz
Physical Layer Details	FHSS 1600 hops per second	Uncoded QPSK, Trellis Coded QPSK or 16/32/64-QAM scheme	DSSS with BPSK or MSK (D-QPSK)
Channel Access	Master - Slave Polling, Time Division Duplex (TDD)	CSMA-CA, and Guaranteed Time Slots (GTS) in a Superframe structure	CSMA-CA, and Guaranteed Time Slots (GTS) in a Superframe structure
Maximum Data Rate	Up to 1 Mbps	11-55 Mbps	868 MHz - 20, 915 MHz - 40, 2.4 GHz - 250 kbps
Coverage	< 10 m	< 10m	< 20 m
Power Level Issues	1 mA – 60 mA	< 80 mA	Very Low current drain (20-50 μ A)
Interference	Present	Present	Present
Price	Low (< \$ 10)	Medium	Very Low
Security	Less Secure. Uses the SAFER + encryption at the baseband layer. Relies on higher layer security.	Very High level of Security including authentication, privacy, encryption and digital certificate services.	Security features in development.



WLANs versus WPANs

- The only similarity between WPAN and WLAN is that they both are wireless technologies, i.e., their role is to allow the transmission of information between devices by a radio link
- This is something also shared by devices such as cellular phones, walkie-talkies, garage door openers, cordless phones, satellite phones, etc.
- There are several fundamental differences between WPANs and WLANs, such as **range, price, abilities, primary role, power consumption, etc.**
- One of the most important issues is the range
- Figure 5.21 shows the various wireless technologies and their suitability for a given radio coverage and the type of networks
- As we can see, WPAN and WLAN systems have completely different scopes and, hence, distinct applications

WLANs versus WPANs





Conclusions and Future Directions

- **Wireless PANs are also experiencing a considerable growth, but clearly not as much as the explosive growth seen in the wireless LANs arena**
- **Obviously, this is largely due that wireless PANs are much more recent than wireless LANs**
- **Nevertheless, the vast availability of Bluetooth devices and the standardization of IEEE of various WPAN systems will take this field to a new level**
- **There are numerous environments where WPANs are very suitable such as in sensor networks, while in the home and in the office, WPANs will be part of our lives**
- **But before that can be realized, many technical challenges have to be solved**
- **Interference mitigation with other systems operating in the same frequency band, effective QoS support, decentralized network formation, energy conservation and security are just a few examples**